



CENTER FOR TRUSTWORTHY  
SCIENTIFIC CYBERINFRASTRUCTURE



# **Streamlining Collaboration with InCommon and Identity Federations**

Warren G Anderson, Ph.D. (LIGO)

Jim Basney, Ph.D. (CTSC)

# **PART I - *INTRODUCTION***

*“The journey of a thousand miles begins with one step.”*

Lao Tzu

# Research VOs are Collaborations





# VOs Collaborate With VOs

WebHome < Bursts/GWNU x

https://wiki.ligo.org/Bursts/GWNU/WebHome

☆

☰



Jump

Search

**Bursts/GWNU**

You are here: LIGOWiki > Bursts/GWNU Web > WebHome (09 Sep 2013, JessicaMciver)

Edit

Attach

Hello Scott Koranda

**My links:**

- Signing Shib metadata
- MyLIGO development
- Auth Project RT
- Formatting

edit

**Toolbox**

- Create New Topic
- Index
- Search
- Changes
- Notifications
- RSS Feed
- Statistics
- Preferences

**Webs**

- AIC
- AuthProject
- Bursts

## Welcome to the Bursts/GWNU web

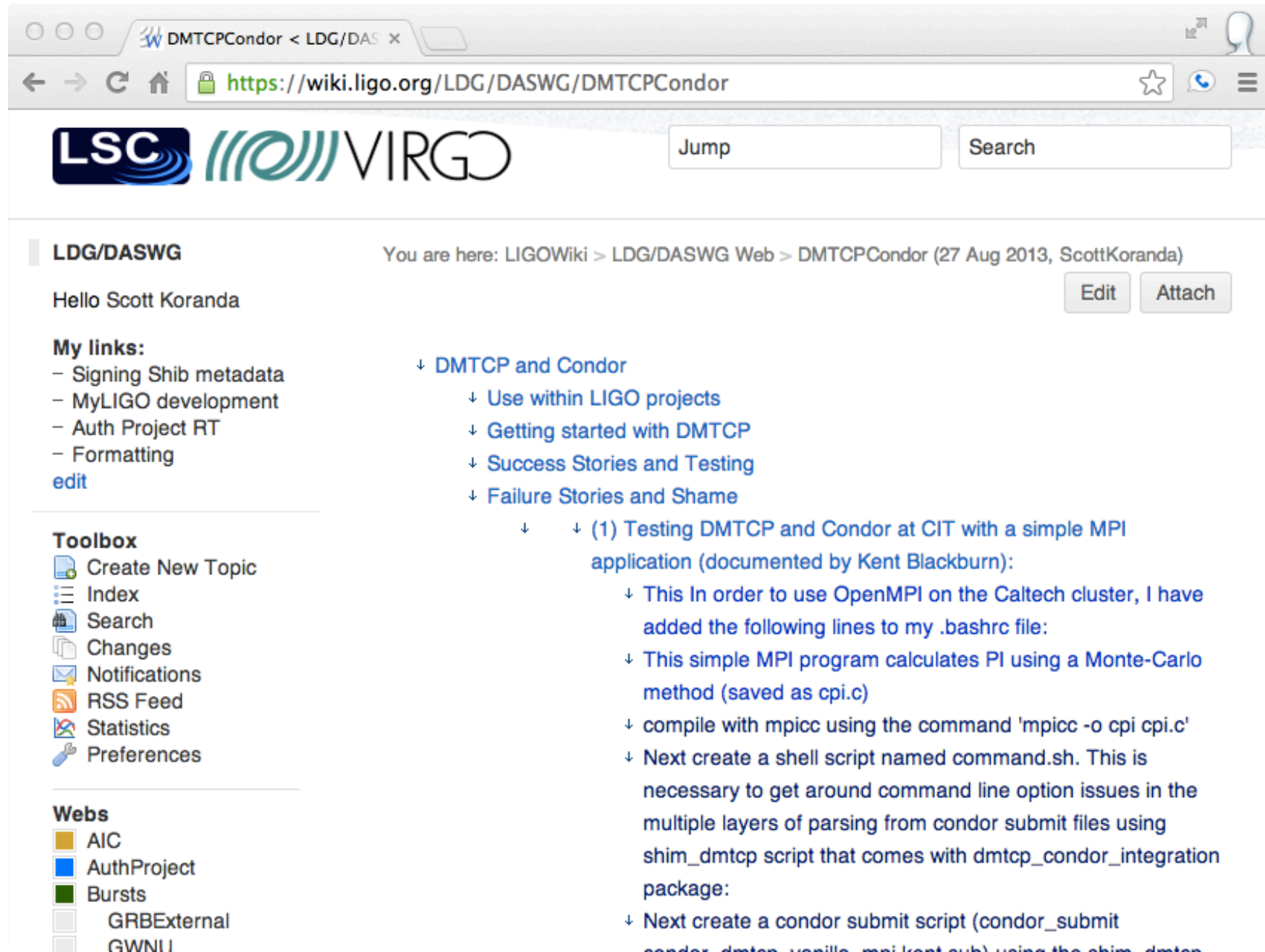
This is the top-level page of the combined search for core-collapse supernovae using neutrino and gravitational waves (GWs). The work is being carried out by a group involved in gravitational waves and neutrino theory, phenomenology and experiment. Institutional representation from LIGO-Virgo (on the gravitational-wave end) and Borexino-Icecube-LVD (on the neutrino end) is present. Beyond these collaborations, colleagues working in other experiments (e.g., KAGRA, Super-Kamiokande) and theory of core-collapse supernovae are also participating. To reach this group via e-mail, use [gwnu@ligo.org](mailto:gwnu@ligo.org) , and/or to reach the burst group of the LIGO-Virgo collaboration, use [bursts@ligo.org](mailto:bursts@ligo.org) .

## Available Information

- [Proposal for collaboration](#)
- LIGO-Virgo and Borexino-Icecube-LVD MoU? (in preparation)
- to-do list for September 2013
  - finalize MoU?
  - establish live times and existing trigger data sets to use on the GW [link](#)



# Support Requires Collaboration



DMTCPCondor < LDG/DAS x

← → ↻ 🏠 🔒 <https://wiki.ligo.org/LDG/DASWG/DMTCPCondor> ☆ ☎ ☰

**LSC** **VIRGO**

**LDG/DASWG** You are here: LIGOWiki > LDG/DASWG Web > DMTCPCondor (27 Aug 2013, ScottKoranda)

Hello Scott Koranda

**My links:**

- Signing Shib metadata
- MyLIGO development
- Auth Project RT
- Formatting

[edit](#)

**Toolbox**

- Create New Topic
- Index
- Search
- Changes
- Notifications
- RSS Feed
- Statistics
- Preferences

**Webs**

- AIC
- AuthProject
- Bursts
- GRBExternal
- GWNI

↓ **DMTCP and Condor**

- ↓ [Use within LIGO projects](#)
- ↓ [Getting started with DMTCP](#)
- ↓ [Success Stories and Testing](#)
- ↓ [Failure Stories and Shame](#)

↓ ↓ (1) Testing DMTCP and Condor at CIT with a simple MPI application (documented by Kent Blackburn):

- ↓ This In order to use OpenMPI on the Caltech cluster, I have added the following lines to my .bashrc file:
- ↓ This simple MPI program calculates PI using a Monte-Carlo method (saved as cpi.c)
- ↓ compile with mpicc using the command 'mpicc -o cpi cpi.c'
- ↓ Next create a shell script named command.sh. This is necessary to get around command line option issues in the multiple layers of parsing from condor submit files using shim\_dmtcp script that comes with dmtcp\_condor\_integration package:
- ↓ Next create a condor submit script (condor\_submit

# Collaboration Often Cumbersome

Too often getting access requires new identity

“Just click here to ask for a new account”

- May take days or weeks for new account
- Frustrates users both inside and outside VO
- Organization “leaks” accounts and access
  - Right now does your VO know who can access what and for how long?

# Enabling Efficient VO Collaboration

What's a science VO to do?

# Google Apps!

My Drive - Google Drive

https://drive.google.com/a/ligo.org/#my-drive

+Scott Search Images Drive Calendar Sites Admin Mobile Photos More -

LIGO

scott.koranda@ligo.org

Drive

CREATE

My Drive

Shared with me

Starred

Recent

More -

Download Drive for Mac

Meet your Drive

My Drive is the home for all your files. With Google Drive for your Mac, you can sync files from your computer to My Drive.

Download Google Drive for Mac

Then, go for a spin

- Explore the left hand nav
- Create Google Docs and
- See files at a glance with
- Get the Google Drive mo

My Drive

<input type="checkbox"/>	TITLE	OWNER
<input type="checkbox"/> ☆	Untitled document Shared	me

0% full

# Google Apps?

Everyone just use Google!

If you can do this then do it...

- Fast to set up
- Easy for users
- Free (as in beer)
- Just works



# Google Apps?

Does not fit all VOs

- Sharing documents isn't the only need
  - Also access to domain specific services and tools
- Real privacy concerns
  - Especially for international collaborations
- As VO grows do does need for infrastructure
  - Google Apps only part of a solution
  - Larger VOs driven to look more “enterprise”

# Science VO IAM

VOs need Identity & Access Management plan

- Enable access to services, tools, and data
- Manage that access to support VO mission
- It's not a data curation plan...
- It's not a cybersecurity plan
- Distinct effort
  - who gets access to what, when, and why
- Federated identity should be important part of plan

## **PART II – *IAM IN A NUTSHELL***

*“Any philosophy that can be put in a nutshell belongs there.”*

Sydney J. Harris

# Definition - Identity

- Your electronic identity
- Information set about you
- Used for
  - authentication  
(who are you)
  - authorization  
(what allowed to do)

`scott.koranda@ligo.org`

Scott

Koranda

Scott F Koranda

14145550208

staff

PO Box 413 Milwaukee, WI

LIGOVirgoLSCMember

# Definition - Access Management

Access Management is about who can access which online resources.

Who is allowed which privileges at which times.

`scott.koranda@ligo.org`  
has privileges VIEW,  
EDIT, RENAME for topic  
AuthProject/WebHome in  
`wiki.ligo.org` from  
January 1, 2013 through  
January 31, 2013



# Identity & Access Management (IAM)

Most people find they collect multiple identities over time, each with its own credentials and privileges.

scott.koranda@ligo.org  
skoranda@uwm.edu  
skoranda  
skoranda@gmail.com  
scott\_koranda@yahoo.com  
scott\_koranda\_ligo (Skype)  
skoranda000 (AIM)  
6310907720 (Delta)  
ScottKoranda (Foswiki.org)  
skoranda (github)  
scott\_koranda (NYTimes)  
Scott Koranda (Facebook)

# **IAM for Scientific Organizations**

Focus here is IAM for scientific organizations.

A primary goal is enabling efficient and secure collaboration to support the science mission of the project.

IAM is successful for science VOs if it increases science opportunity.

## Why bother with IAM?

Larger, even medium size, science projects have tendency to evolve organically rather than by design.

And the user experience often shows it...

## Begins innocently enough...

“We need an email list to make it easier to communicate. Let’s deploy mailman.”



CBC Info Page

www.lsc-group.phys.uwm.edu/mailman/listinfo/cbc

## CBC -- LIGO-Virgo Compact Coalescing Binaries Group

About CBC

English (USA)

This is the mailing list of the LIGO-Virgo joint working group search for gravitational waves from compact binary coalescence.

To see the collection of prior postings to the list, visit the [CBC Archives](#). *(The current archive is only available to the list members.)*

Using CBC

To post a message to all the list members, send email to [cbc@gravity.phys.uwm.edu](mailto:cbc@gravity.phys.uwm.edu).

You can subscribe to the list, or change your existing subscription, in the sections below.

Subscribing to CBC

Subscribe to CBC by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscribing you. Once confirmation is received, your request will be held for approval by the list moderator. You will be notified of the moderator's decision by email. This is also a private list, which means that the list of members is not available to non-members.

Your email address:

Your name (optional):

You may enter a privacy password below. This provides only mild security, but should prevent others from messing with your subscription. **Do not use a valuable password** as it will occasionally be emailed back to you in cleartext.

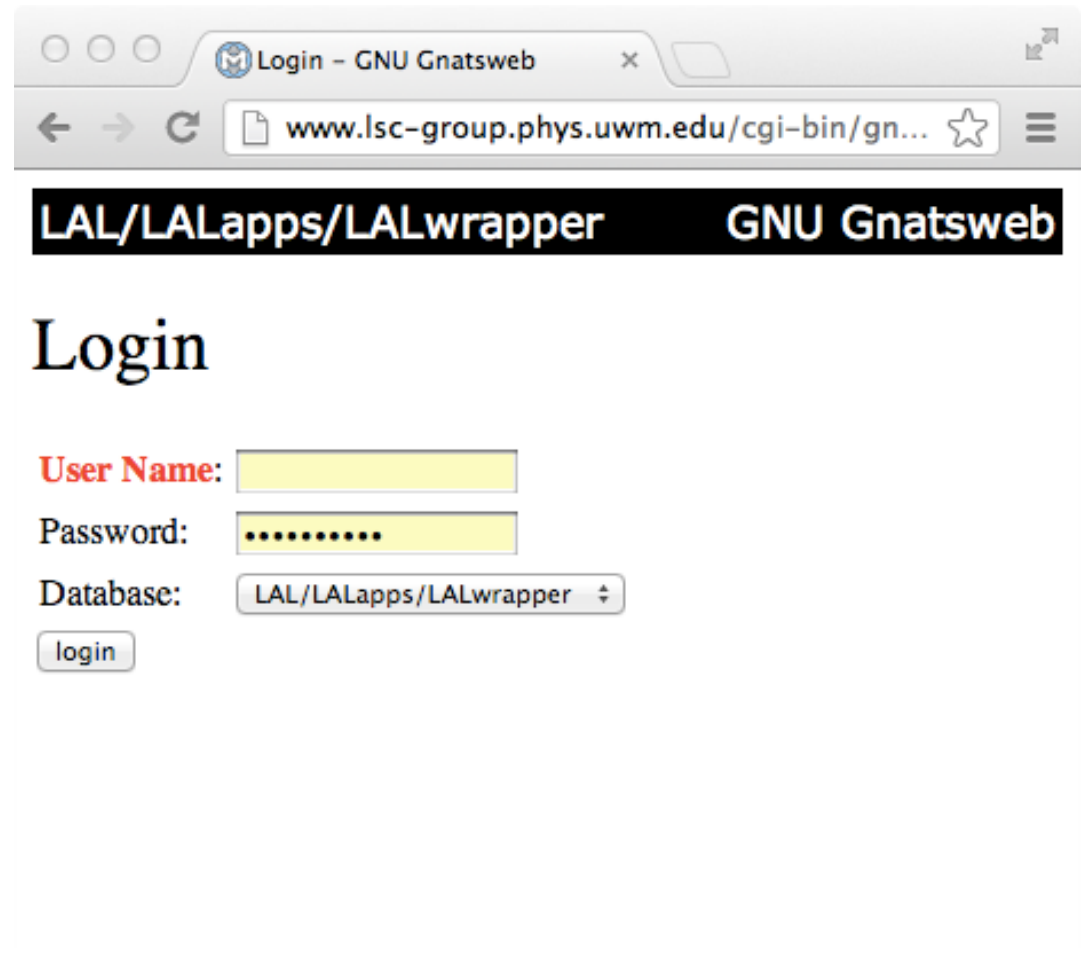
If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription. You can always request a mail-back of your password when you edit your personal options. Once a month, your password will be emailed to you as a reminder.

Pick a password:



## More tools follow...

“We need a bug tracking system to track all these issues!”



The screenshot shows a web browser window with the title "Login - GNU Gnatsweb". The address bar displays the URL "www.lsc-group.phys.uwm.edu/cgi-bin/gn...". Below the browser window, there is a black navigation bar with the text "LAL/LALapps/LALwrapper" and "GNU Gnatsweb". The main content area is titled "Login" and contains a form with the following fields:

- User Name:** A text input field.
- Password:** A password input field with masked characters (dots).
- Database:** A dropdown menu showing "LAL/LALapps/LALwrapper".
- login**: A button to submit the login information.

# Still more tools...

“Editing HTML is too hard. We need a wiki.”

The screenshot shows a web browser window with the address bar displaying `https://gravity.astro.cf.ac.uk/dokuwiki/start?do=register`. The page header includes the Cardiff University logo, the title 'Gravitational Physics', and navigation links for 'Register', 'Login', 'Recent changes', 'Media Manager', and 'Sitemap'. A search bar is also present. The main content area is titled 'Register as new user' and contains instructions: 'Fill in all the information below to create a new account in this wiki. Make sure you supply a **valid e-mail address** - if you are not asked to enter a password here, a new one will be sent to that address. The login name should be a valid [pagename](#).' Below the text is a registration form with fields for 'Username', 'Real name', and 'E-Mail', and a 'Register' button. The footer of the page indicates the file is 'start.txt' and was last modified on 2012/12/28 at 13:30 by duncan.macleod@LIGO.ORG.

# Geographic Issues

Diverse groups makes the issue worse.

“We’re not used to Moin, our lab uses Twiki”

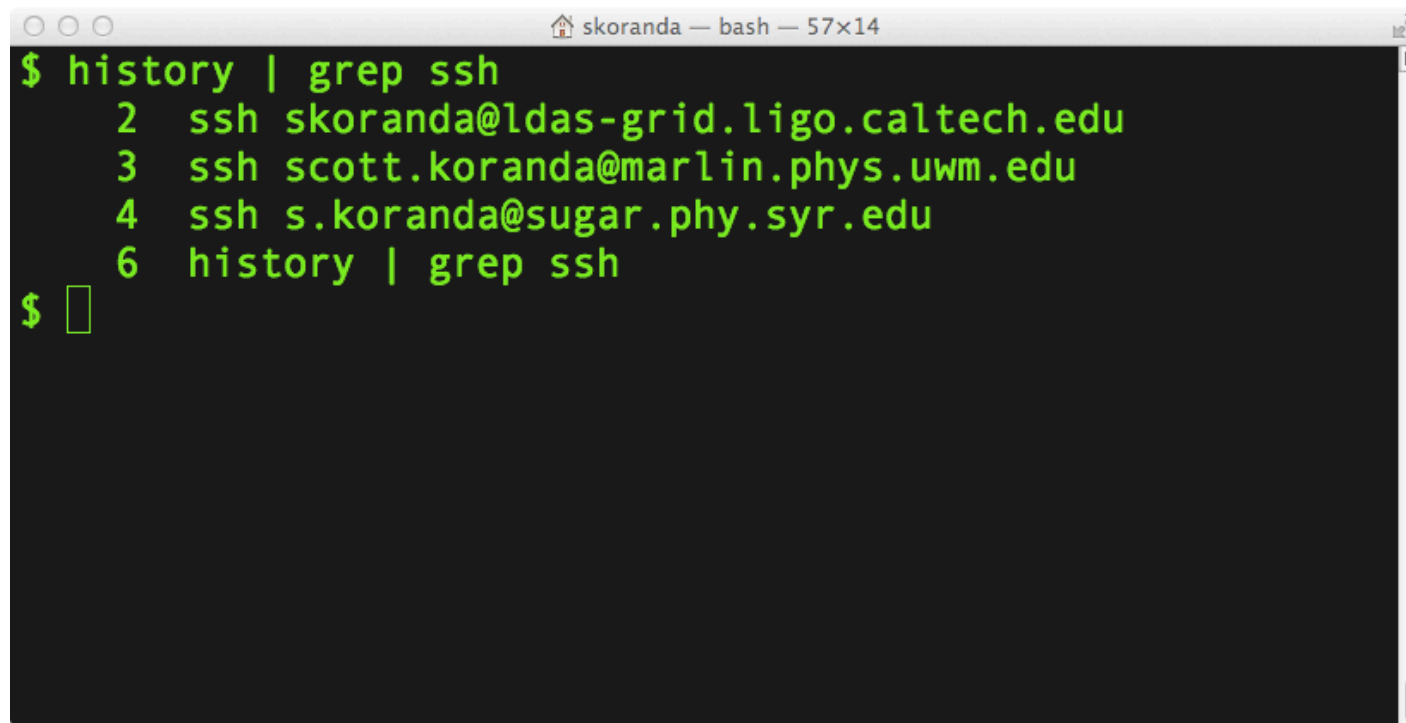
“What’s Twiki? Our university uses Dokuwiki”

“Dokuwiki is too complicated, we use MediaWiki”

“I don’t like MediaWiki, so I wrote my own!”

# Command Line Tools

This is not just a “port 80/443” problem...

A terminal window titled 'skoranda — bash — 57x14' with a dark background and green text. The user has entered the command '\$ history | grep ssh'. The terminal displays the following history entries:

```
$ history | grep ssh
 2  ssh skoranda@ldas-grid.ligo.caltech.edu
 3  ssh scott.koranda@marlin.phys.uwm.edu
 4  ssh s.koranda@sugar.phy.syr.edu
 6  history | grep ssh
$
```

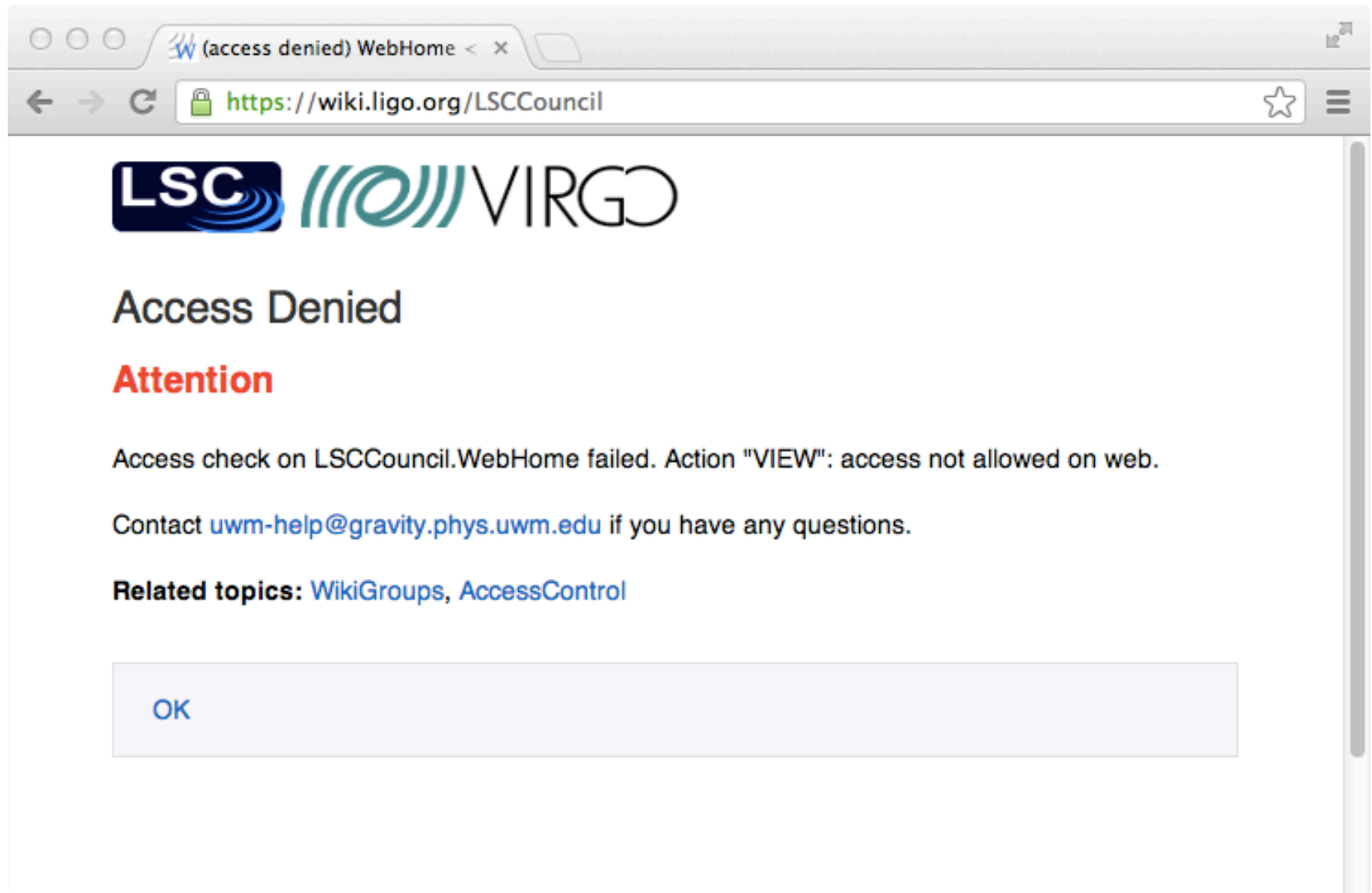
# Access Management

Science VO management structure generally much flatter than Enterprise or Higher Ed.

Eventually access privileges are no longer “flat.”

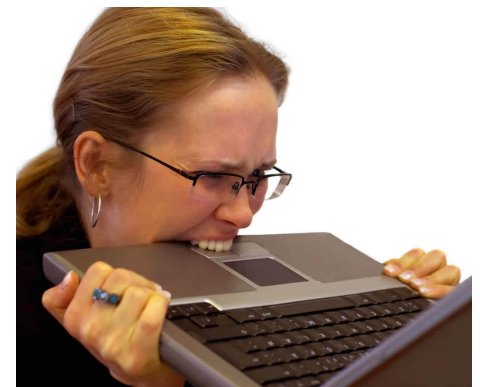
Some things some people can see or do...  
...other things other people can see or do.





# Users Frustrated

- Eventually the burden is too high on users.
  - Too many accounts/logins/passwords.
  - Too many places to manage them.
- Drives insecure online behavior.
- Collaboration efficiency suffers.



Copyright unknown

# Organizational Dysfunction

“I need a list of all people in the collaboration!”

- No such list exists
- List is not up to date
- List is inaccessible to people that need it

# Organizational Dysfunction

From: admin@bigproject.org  
To: users@bigproject.org  
Subject: Fwd: where do I login?

Anybody know who this person is? Should she have an account?

> From: jane.scientist@university.edu  
> To: admin@bigproject.org  
> Subject: where do I login?  
>  
> I just joined Big Project and was told that you could help me get  
> an account?

# Organizational Dysfunction

From: jane.scientist@univeristy.edu  
To: admin@bigproject.org  
Subject: Fwd: minutes from last meeting

Please remove me from this list. I have not been a part of Big Project for over 2 years now!

> From: dyoung@somewhere.edu  
> To: users@bigproject.org  
> Subject: minutes from last meeting  
>  
> The minutes from the last meeting are attached. Sorry about  
> the size. I don't know how to make the imported diagrams  
> any smaller. Let me know if your email can't handle attachments  
> more than 2 gigabytes.

# IAM for Science

What makes IAM for science projects unique?

- Mixture of web and command line tools.
- Often geographically distributed.
- Often decentralized organizational structure.
- Often fewer lines of authority.
- Underfunded and not enough people resources.
- “Let’s just do it and get it done” culture.

Smart and technology savvy people +  
little structure = infrastructure “challenges”

# IAM for Science

Good news is that there is help:

- Technology **can** help.
- Good open source standards-based tools with strong communities available.
- Flexible, loosely coupled design goes long way.
- Leverage experience from other organizations.
  - especially campuses

# IAM for Science

Bad news is that there is no silver bullet:

- Technology can only do so much.
- Policy drives the technology.
- Organizations need to articulate policies that can be implemented and expressed by the tools.
- Scientists do not like to spend time thinking through and enumerating the fine details of policy.
- Physicists particularly bad because they want to abstract the problem and find universal expressions.

Resulting policy is complex and ugly.



# **IAM for Science**

Need to begin policy discussions early in parallel with technology design.

Drive conversations with use cases.

Iterate quickly, stand up demonstration services, help busy scientists focus on policy questions.

## **PART III - *IAM Model Components***

*“Divide each difficulty into as many parts as is feasible and necessary to resolve it.”*

Rene Descartes

# IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service providers
- Group, role, and privilege manager
- Attribute authority

# IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

# **IAM Component: User Registry**

- Holds records of users or members
- Portal for users to self-manage identity
- Portal for credential (password) management
- Enrollment or “onboarding” new members
- Management of “offboarding”
- Also often reporting functions
- Also often interface into other components

myLigo x

← → ↻ <https://my.ligo.org> ☆ ☰

my Ligo News Roster Support

Welcome!

Please **Sign In**

LIGO Email Address:  @ LIGO.ORG

Password:

[\(Forgot Your Password?\)](#)

Login

or **Register** for a LIGO account

Please choose one of these three ways to register:

Start here if you are affiliated with a LIGO Scientific Collaboration (LSC) site or you are a Virgo Collaboration member, but are not affiliated with a LIGO Lab site.


LSC or Virgo Sign Up


Start here if you are affiliated with a LIGO Lab site (Caltech, Hanford, Livingston, MIT).

LIGO Lab Sign Up

Start here if you are serving on an external committee.

External Committee Sign Up

 LIGO Directory Services and Authentication & Authorization Services Infrastructure are supported by the [National Science Foundation](#). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.



myLigo

https://my.ligo.org/adduserLVC.php

# my Ligo

## Account Application

### Describe LIGO Affiliation

**\*Please select one option:**

☐ I am an [LSC member](#)  
at

☐ I am not an LSC member but provide administrative support for an LSC group  
for

☐ I am a Virgo member

### Name

**\*First Name:**

**Middle Name:**

**\*Last Name:**

**Suffix:**

myLigo

https://my.ligo.org/myinfo.php?do=cont

my Ligo

News

Edit My Personal Information

My Information Manage Group

**Actions:**

- [Edit My Contact Information](#)
- [My @LIGO.ORG Info](#)
- [Demographics](#)
- [Demographics Report](#)
- [Census Report](#)

**Update My Business Contact Information**

Please Select an Affiliation: LSC - UW Milwaukee

**LSC - University of Wisconsin - Milwaukee**

Office Address 1: UWM Physics Department

Office Address 2: P.O. Box 413

Office Address 3:

City: Milwaukee State: WI

Postal Code: 53201

Country: (Please begin by selecting one of the following Continents)

☒ North America ☐ Europe ☐ Asia ☐ South America

☐ Africa ☐ Oceania ☐ Antarctica



# User Registry Design

Design?

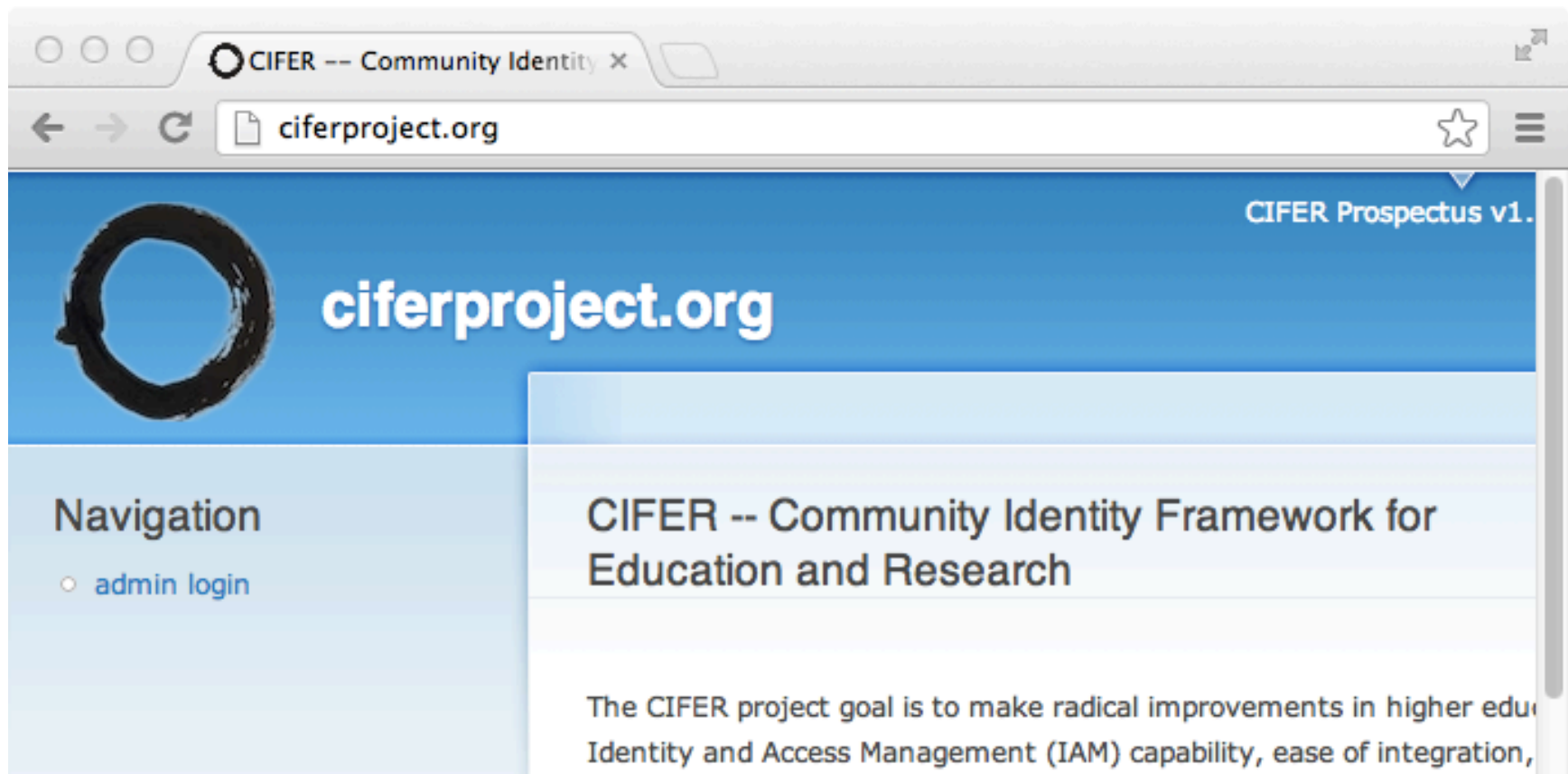
Are there not all-in-one tools to download and use?

No (mostly).

Existing enterprise solutions too heavyweight and inflexible for science organizations.

LIGO currently using homebrewed solution.

# Projects to Watch



# Projects to Watch

Manage Identities | Account x

https://www.globusonline.org/account/ManageIdentities

globus online Manage Data | Groups | Support | skoranda

update profile | change password | account privacy | group membership | manage identities

## Manage Identities

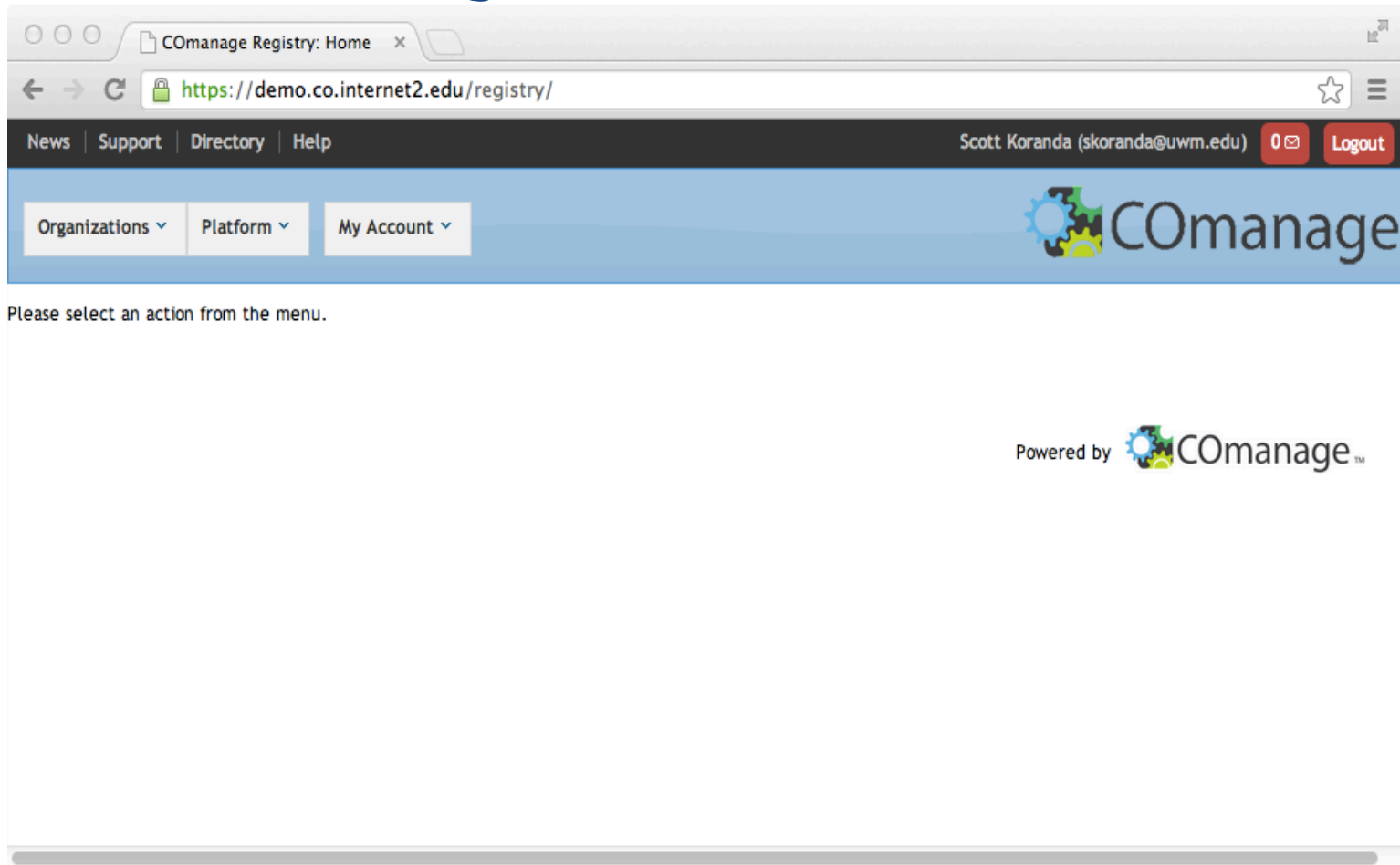
Add External Identity Add X.509 Certificate Add SSH Public Key

Alias	Type	Authentication Provider			
system-generated openid alias	openid	google.com	View Details	Update	Delete
DOEGrids	x509	CN=DOEGrids CA 1...	View Details	Update	Delete

Add External Identity Add X.509 Certificate Add SSH Public Key

Support

# Projects to Watch



# LIGO Uses CManage

COmanage Registry: CO People

[https://gw-astronomy.org/registry/co\\_people/index/co:2/sort:status/direction:asc](https://gw-astronomy.org/registry/co_people/index/co:2/sort:status/direction:asc)

News | Support | Directory | Help

Scott Koranda (scott.koranda@ligo.org) 0 Logout

Organizations Platform My Account

**KAGRA-LIGO People**

Name	Status	Roles	Actions
<a href="#">Steve Koranda</a>	Active	<a href="#">member</a>	<a href="#">Add</a> <a href="#">Edit</a>
<a href="#">Eiichi Hirose</a>	Active	<a href="#">member</a>	<a href="#">Add</a> <a href="#">Edit</a>
<a href="#">Shinji Miyoki</a>	Active	<a href="#">member</a>	<a href="#">Add</a> <a href="#">Edit</a>
<a href="#">Yusuke Sakakibara</a>	Active	<a href="#">member</a>	<a href="#">Add</a> <a href="#">Edit</a>
<a href="#">Osamu Miyakawa</a>	Active	<a href="#">member</a>	<a href="#">Add</a> <a href="#">Edit</a>
<a href="#">Takanori Sekiguchi</a>	Active	<a href="#">member</a>	<a href="#">Add</a> <a href="#">Edit</a>
<a href="#">Masahiro Kamiizumi</a>	Active	<a href="#">member</a>	<a href="#">Add</a> <a href="#">Edit</a>

+ Enroll

# COnanage

## Collaborative Organization Management

- A collaboration management platform.
- Joint project with Internet2 and iPlant.
- NSF funded.
- Supports flexible enrollment and management for federated identities.
- Provisions into attribute authority.

# Collaboration Management Platforms

- CManage (I2, LIGO, iPlant)
- OpenConext from SURFnet (NL)
- Many federations host CMP for VOs:
  - SWiTCH (CH)
  - GakuNin (JP)
  - Perun (CZ)
- Globus Online (?)

# User Registry Design

**Data types** - What data will be stored?

**Data Store** - What backend data store?

**Onboarding** – How do new users get registered?

**Offboarding** – How to decommission accounts?

**Reporting** - What summary or metadata is needed?



# User Registry Design

## Data Types

What data does your project need?

givenName  
familyName (sn)  
common name (cn)  
displayName  
preferredName  
honorific  
suffix  
mail  
mailForwardingAddress  
mailAlternateAddress  
address

telephone  
eduPersonPrincipalName  
eduPersonOrgDN  
eduPersonAffiliation  
eduPersonEntitlement  
isMemberOf  
title  
openID  
uid  
gid  
...

# User Registry Design

## Data Types

Only collect and store the data you need to accomplish the organization's mission.

Do not collect data because you “might use it someday”.

Instead, design flexibility to add data types as needed.

# User Registry Design

## Data Types

Be sure to look at the eduPerson LDAP schema

Other resources:

- Other science projects
- CIFER, Kuali IdM, COmanage
- Your campus IT staff

# User Registry Design

## Data Types

Whether your registry *provisions* (is a source of) identity or *consumes* (federated) identity affects which data types to collect and store.

# User Data Registry Data Store

First question is usually SQL or LDAP?

SQL:

- More flexibility—create the tables you need.
- Integrates easily with MVC web frameworks.
  - model, view, controller
  - Django, CakePHP, Catalyst

LDAP:

- More standards—leverage existing schemas.
- Easy replication for redundancy.
- Easy integration with large number of tools.
  - pam\_ldap for integration into shell

# User Data Registry Data Store

SQL or LDAP?

For small projects with limited IAM needs LDAP more likely for bootstrapping infrastructure.

For larger projects use both SQL and LDAP:

- SQL as the primary data store.
- Reflect into LDAP for replication, consumption by other tools including attribute stores.

# User Registry Onboarding

Onboarding: how people enter into the IAM infrastructure.

- Usually coming new into the project.
- Sometimes returning to the project.
- May have different policies:
  - per person affiliation (faculty, staff, student, ...)
  - per organization unit
  - as project grows and matures

# User Registry

## Offboarding

Offboarding: how people leave the IAM infrastructure.

- Always last part considered and designed!
- Usually involves decrease in privileges over time.
- May have different policies ...
  - ... per person affiliation (faculty, staff, student, ...)
  - ... per organization unit
  - ... as project grows and matures

“We need postdocs to have read and write permissions to the paper database for one year after they leave the project.”



# User Registry Reporting

As size of project grows management will ask for increasingly complex views of the user registry.

Demographics, especially in the US, important to funding agencies.

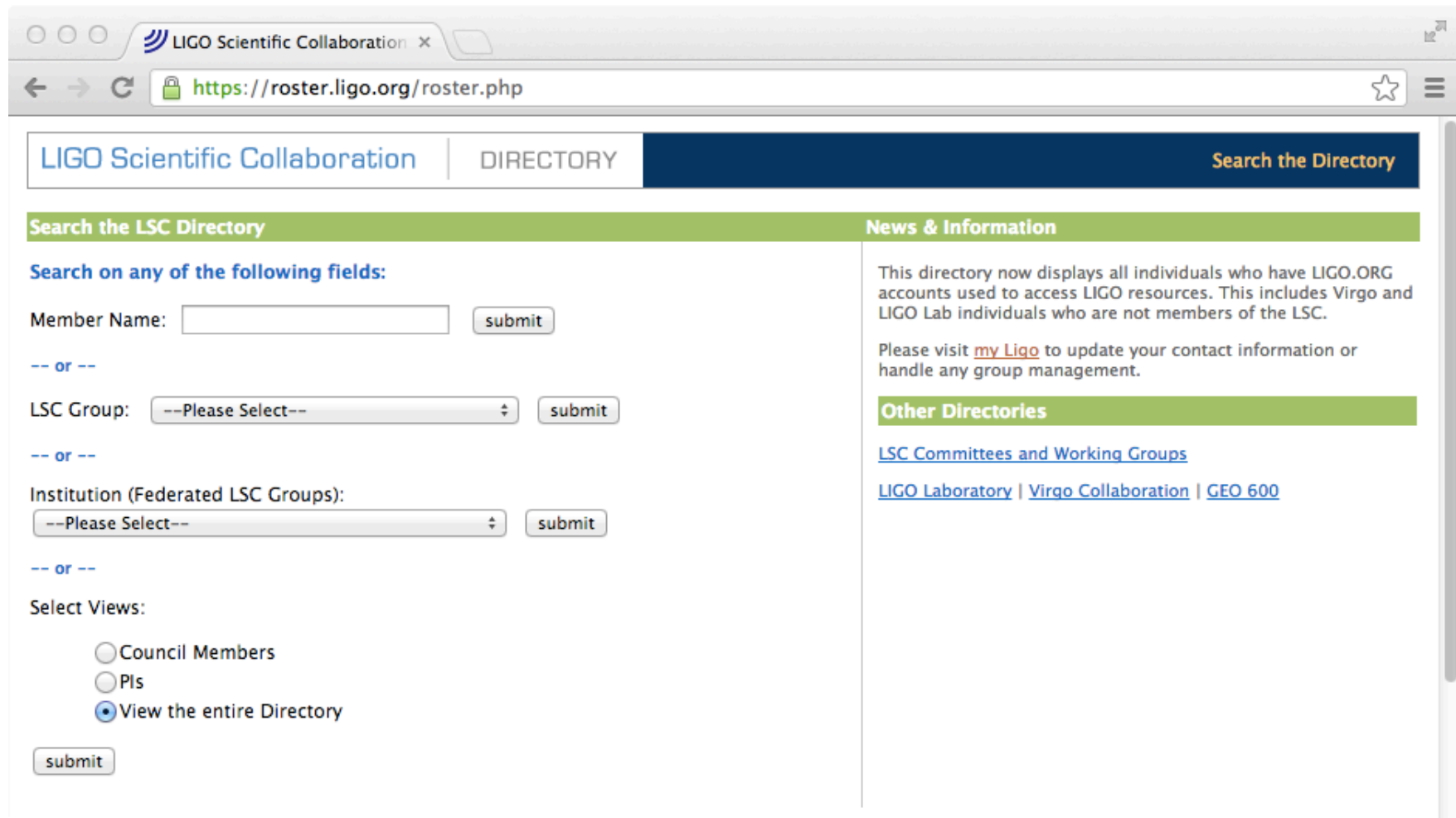
“How many female graduate students joined the project between 2010 and 2012?”

# IAM Components

- User registry
- **Directory**
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

# IAM Component: Directory

Directory/Roster often first reporting from registry.



The screenshot shows a web browser window with the address bar displaying <https://roster.ligo.org/roster.php>. The page header includes the LIGO Scientific Collaboration logo, the word "DIRECTORY", and a "Search the Directory" button. The main content area is divided into two columns. The left column, titled "Search the LSC Directory", contains search fields for "Member Name", "LSC Group", and "Institution (Federated LSC Groups)", each with a "submit" button. Below these are radio buttons for "Select Views": "Council Members", "PIs", and "View the entire Directory" (which is selected). A "submit" button is at the bottom of this column. The right column, titled "News & Information", contains text about the directory's scope and a link to "my Ligo". Below this is a section titled "Other Directories" with links to "LSC Committees and Working Groups", "LIGO Laboratory", "Virgo Collaboration", and "GEO 600".

LIGO Scientific Collaboration | DIRECTORY | Search the Directory

**Search the LSC Directory**

Search on any of the following fields:

Member Name:  submit

-- or --

LSC Group: --Please Select-- submit

-- or --

Institution (Federated LSC Groups):  
--Please Select-- submit

-- or --

Select Views:

☐ Council Members  
☐ PIs  
☒ View the entire Directory

submit

**News & Information**

This directory now displays all individuals who have LIGO.ORG accounts used to access LIGO resources. This includes Virgo and LIGO Lab individuals who are not members of the LSC.

Please visit [my Ligo](#) to update your contact information or handle any group management.

**Other Directories**

[LSC Committees and Working Groups](#)  
[LIGO Laboratory](#) | [Virgo Collaboration](#) | [GEO 600](#)

## Directory/Roster

Although a “view” of the registry consider making a distinct component.

- Use a separate data store.
- Provisioned by the registry.
- Only provision subset data needed.

Help protect against PII (Personally Identifiable Information) leaks.

LIGO uses stand-alone openLDAP instance.

# IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

# **IAM Component: Authentication Store**

If you provision identity and with it an identifier (login) and a credential (e.g. password) used for authentication you need an authentication store.

Usual candidates:

- SQL
- LDAP
- Kerberos KDC
- Active Directory
- Shadow files

# Authentication Store

Choice for authentication store depends on:

- Tools and services that need to leverage it.
  - web apps, shells, thick client, ...
- Organizational security tolerances.
  - Can passwords go over the network?
  - Over protected channels?
- Operational team experience and depth.

# LIGO Authentication Store

LIGO chose Kerberos

- MIT implementation.
- Single master KDC with many slave replicas.
- Standard ports (88) and 80/443
  - Firewall traversal out of hotels for example.
- Integrated with DNS
  - Clients need no special configuration.
- Use web interface to manage password.
  - More friendly for most users.
  - Some users use command line.



# LIGO Authentication Store

Kerberos principal is the primary LIGO identifier

- albert.einstein@LIGO.ORG
- LIGO.ORG is the Kerberos realm.
- LHO (soon LLO, CIT) have their own realms.
- Use cross-realm trust configuration for smooth integration.

# Authentication Store

Especially with SSO, credentials are “keys to the kingdom.”

Get input from a real security expert!

IAM and security complimentary but distinct.

- Security officer has skills, training, and experience IAM architects should leverage.

Cultivate a working relationship early in design phase with your security expert.

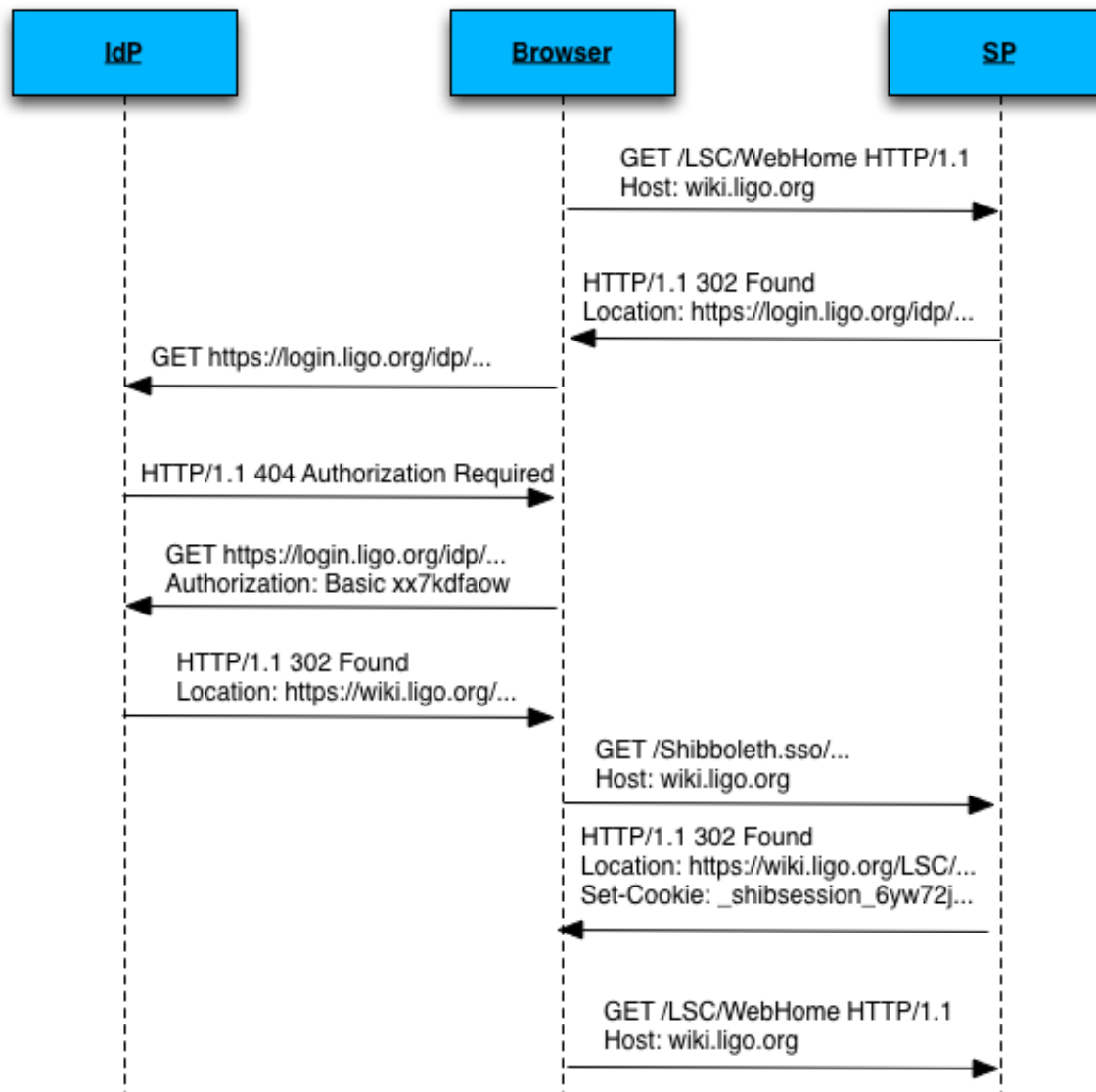
# IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

# **IAM Component: Identity Provider**

Identity Provider (IdP) asserts identity:

- To a third-party service provider (SP).
- Usually after an authentication event.
- Usually across a security or identity domain.
  - Still useful concept within an identity domain.
- Most often used in web context.
  - But the concept applies more generally.



# IdP

IdP authenticates the user and sends back to SP.  
IdP asserts that the user has authenticated.

- Often includes some details about how.
- Often includes some details about when.
- Usually asserts an identifier for the user.
  - may be *opaque* and/or *targeted*.
- Sometimes asserts attributes about user.

Details depend on format chosen by IdP and SP.

# Web AuthN/Z Protocols

## OpenID:

- Relatively simple.
- Supported by Google, FB, Twitter, Yahoo, ...
- Good adoption in web 2.0 spaces.
- Not focused on preserving privacy.
- Not focused on rich attribute exchange.
  - OpenID Authentication 2.0 and OpenID Attribute Exchange 1.0 helped improve that.

# Web AuthN/Z Protocols

OAuth:

- Focused on authorization, not authentication.
- Type of limited delegation.
- Allow site A (Facebook) to access site B (Instagram) on your behalf.



# Web AuthN/Z Protocols

## OpenID Connect:

- Next generation OpenID.
- Builds on top of and incorporates OAuth 2.
- More complex but delivers more functionality.
- Tension between enterprise needs and “simple”.
- Slow uptake at this moment...

# Web AuthN/Z Protocols

## SAML:

- More complex than OpenID.
- Strong privacy preserving.
- Strong attribute exchange.
- Good adoption in higher education.
- Limited adoption outside of higher education.
  - More uptake in research space recently.

# LIGO Chose SAML

- Strong support from higher education.
  - Strong support from Internet2.
  - Strong support from InCommon.
- Rich attribute assertion mechanisms
  - Less concerned with privacy preservation.
- Straightforward path away if necessary:
  - “Social2SAML” gateways.
  - Allow slow transition if necessary.

# LIGO SAML & Shibboleth

LIGO has significant investment in Shibboleth.

- IdP is Shibboleth 2.3.x.
- Over 60 Shibboleth SPs now.
- Member of the Shibboleth consortium.
- Currently 5+ staff with Shibboleth training.





Shibboleth is an implementation of SAML.

- Originally started by Internet2 in US.
- Now funded by its own consortium.
  - Support both in Europe and US.
- Provides:
  - Identity Provider (Java servlet).
  - Service Provider (Native C Apache module).
  - Centralized or Embedded Discovery Service.

# SAML Tools

- SimpleSAMLphp.
  - open source.
  - both IdP and SP functionality.
  - primarily a European project.
- OpenAM
  - IdP.
  - evolution of OpenSSO from Sun/Oracle.
  - open source with support from ForgeRock.
- Ping Identity
  - private company.
  - IdP.



# IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

# **IAM Component: Service Provider**

Term “service provider” (SP) most often used in web context.

Any service or tool (resource) users or their delegates access.

Access to the SP usually requires authentication *and* authorization.



LIGO Document Control Center

<https://dcc.ligo.org/cgi-bin/private/DocDB/DocumentDatabase>

**LIGO**  
DCC [Home] [Reserve Number] [Search] [Recent Changes] [List Topics] [List Events] [Public Site] [Help]

This is the repository of LIGO talks, publications, and other documents.

[Instructions](#)

[Your Account](#)

[Preferences](#)

[DCC Statistics](#)

[Using the DCC](#)

**List of frequent searches:**

Author **Scott Koranda**

Title

Number **LIGO-**  **-v**

Recent Changes in the last  days.

Basic

Advanced **specify detailed search criteria**

**List documents by:**


- ◇ [Author](#)
- ◇ [Topic](#)
- ◇ [Group](#)
- ◇ [Event](#)

[Event calendar](#) (select date to create a new event)

WebHome < Main < LIGOWiki x

https://wiki.ligo.org

PUBLIC

**LSC**  **VIRGO**

Jump Search

**Main**









Hello Scott Koranda

**My links:**


- Signing Shib metadata
- MyLIGO development
- Auth Project RT
- Formatting

edit

**Main Web**

-  Create New Topic
-  Index
-  Search
-  Changes
-  Notifications
-  RSS Feed
-  Statistics
-  Preferences

**Webs**

-  AIC

You are here: LIGOWiki > Main Web > WebHome (24 Jan 2013, ScottKoranda) Edit Attach

## Welcome to the LIGO/Virgo wiki

Please click "Log In" to see all topics available to LIGO/Virgo community members.

The purpose, access requirements, and a link to the privacy policy [may be found here](#).

Edit | Attach | Print version | History: r4 < r3 < r2 < r1 | Backlinks | View wiki text | Edit wiki text | More topic actions

Topic revision: r4 - 24 Jan 2013, ScottKoranda

```
skoranda — skoranda@oregano: ~ — ssh — 80x24
Scotts-MacBook-Air:~ skoranda$ gsissh ldas-pcdev4.ligo.caltech.edu
Last login: Sun Feb 10 04:01:12 2013 from 119.226.189.166
*****
Welcome to the LIGO-Caltech Computing Cluster
*****
Kickstart-installed Scientific Linux v6.1 Tue Nov 15 14:56:57 PDT 2011

ldas-grid.ligo.caltech.edu      Primary production submit machine
ldas-pcdev1.ligo.caltech.edu    Large memory development and post-processing
ldas-pcdev2.ligo.caltech.edu    Even larger memory devel & post-processing w/GPU
ldas-pcdev3.ligo.caltech.edu    Local user submit machine
ldas-pcdev4.ligo.caltech.edu    Bleeding edge pre-release software
ldas-pcdev5.ligo.caltech.edu    Over-the-edge pre-release software
ldas-pcdev6.ligo.caltech.edu    RHEL6 Over-the-edge pre-release software
*****
python-lxml-2.2.3-1.1.el6 installed (Dec 04)
python-voeventlib-*-0.3-1.lscsoft installed (Dec 04)
bind-*-9.8.2-0.10.rc1.el6_3.6 updated (Dec 10)
ldas-tools-*-1.19.25-1 updated (Dec 10)
mysql-*-5.1.66-2.el6_3 updated (Dec 10)
gds-*-2.16.5-3 updated (Dec 14)
gstlal-*-0.5.0-1.lscsoft updated (Dec 14)
gstlal-inspiral-*-0.1.0-1.lscsoft installed (Dec 14)
gstlal-ugly-*-0.4.0-1.lscsoft updated (Dec 14)
```

# IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

# **IAM Component: Groups, Roles, Privileges Manager**

Access management often maps to **groups**.

“Only members of the ‘executive committee group’ may read and edit the ExComm web at [wiki.ligo.org](http://wiki.ligo.org)”

```
Set ALLOWWEBVIEW =  
Communities:LVC:LSC:ExecComm:ExecCommGroupMembers
```

# Groups, Roles, Privileges Manager

Access management also often maps to **roles**.

- Role-Based Access Control (RBAC).

“The Director of LIGO and the LIGO Scientific Collaboration Spokesperson may download this document from the document control center (DCC).”

# Groups, Roles, Privileges Manager

Many tools include their own groups, roles, and privileges management capabilities.

- Often these offer only limited functionality.
- Not possible to share across organization.

Centralized (specialized) tools for group, role, privilege management:

- LDAP (and tools built on top of it)
- VOMS
- Grouper

# Groups, Roles, Privileges Manager

What to look for in centralized groups/roles/privileges tool:

- Set math.
  - compose, complement.
- No imposed hierarchy.
  - Should not assume a tree hierarchy.
  - No assumptions about organizational structure.
- Time management.
  - Effective dates and times.
  - Auditing (point-in-time).
- Manage entities and objects—not just people.



# Grouper

- Internet2 in the United States.
- Support for set math.
  - both composition and complement.
- No imposed structure.
- Reflection (provisioning) into LDAP.
- Manage groups, roles, and privileges.
  - RBAC support.



# Grouper

- Support for time management:
  - Effective dates/times.
  - Point-in-time auditing.
- Strong support for delegation.
  - Let group leaders manage their own memberships.
- Java servlet with relational database backend.
- Significant learning curve.



LIGO groups manager

https://grouper.ligo.org/grouper/browseStemsAll.do?currentNode=4f9bc5bc-...

**LIGO**

**LSC**

Welcome Scott Koranda Act as admin Change

**My tools**

**Explore**

Search

Folder workspace

Group workspace

Entity workspace

Group types

Help

**LIGO**

Roster

**EXPLORE**

### Browse groups hierarchy

You can look for groups throughout the hierarchy.  
(You might not be able to see some groups if you lack appropriate privileges.)

#### Browse or list groups

**Current location is:**  
 Root: Communities: LVC: LIGOLab

Showing 1-11 of 11 Items

- CIT
- DCC
- External
- Instrumental
- LHO
- LLO
- MIT
- Safety
- DirectorGroupMembers
- LIGOLabGroupManagers
- LIGOLabGroupMembers

LIGO group management based on Grouper from

# IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

# IAM Component: Attribute Authority

Attribute Authority (AA) asserts attributes and attribute values.

```
scott.koranda@ligo.org:  
  givenName: Scott  
  sn: Koranda  
  eduPersonAffiliation: member  
  isMemberOf: LIGO
```

# Attribute Authority

Most often attributes of people.

- But could be attributes about other entities.

Question of which source is authoritative for which attributes is an open research question.

# Attribute Authority

Question of which source is authoritative for which attributes is an open research question:

- LIGO AA asserts `scott.koranda@ligo.org` is a member of LIGO group
- KAGRA AA asserts `yoichi.aso@kagra.org` is a member of KAGRA group
- Who asserts `scott.koranda@ligo.org` and `yoichi.aso@kagra.org` are members in the joint LIGO-KAGRA working group?

# Attribute Authority

Common AA stores or services:

- LDAP
  - Easy integration with spectrum of clients.
  - Solid open source implementations.
- Shibboleth IdP
  - Attribute assertion with authentication event.
  - Attribute assertion without authentication event.
    - Standalone AA functionality.



## **PART IV – *Federated Identity***

*“I am Pavel Chekov, a commander in Starfleet. United Federation of Planets  
Service Number 656-5827D.”*

Star Trek IV: The Journey Home

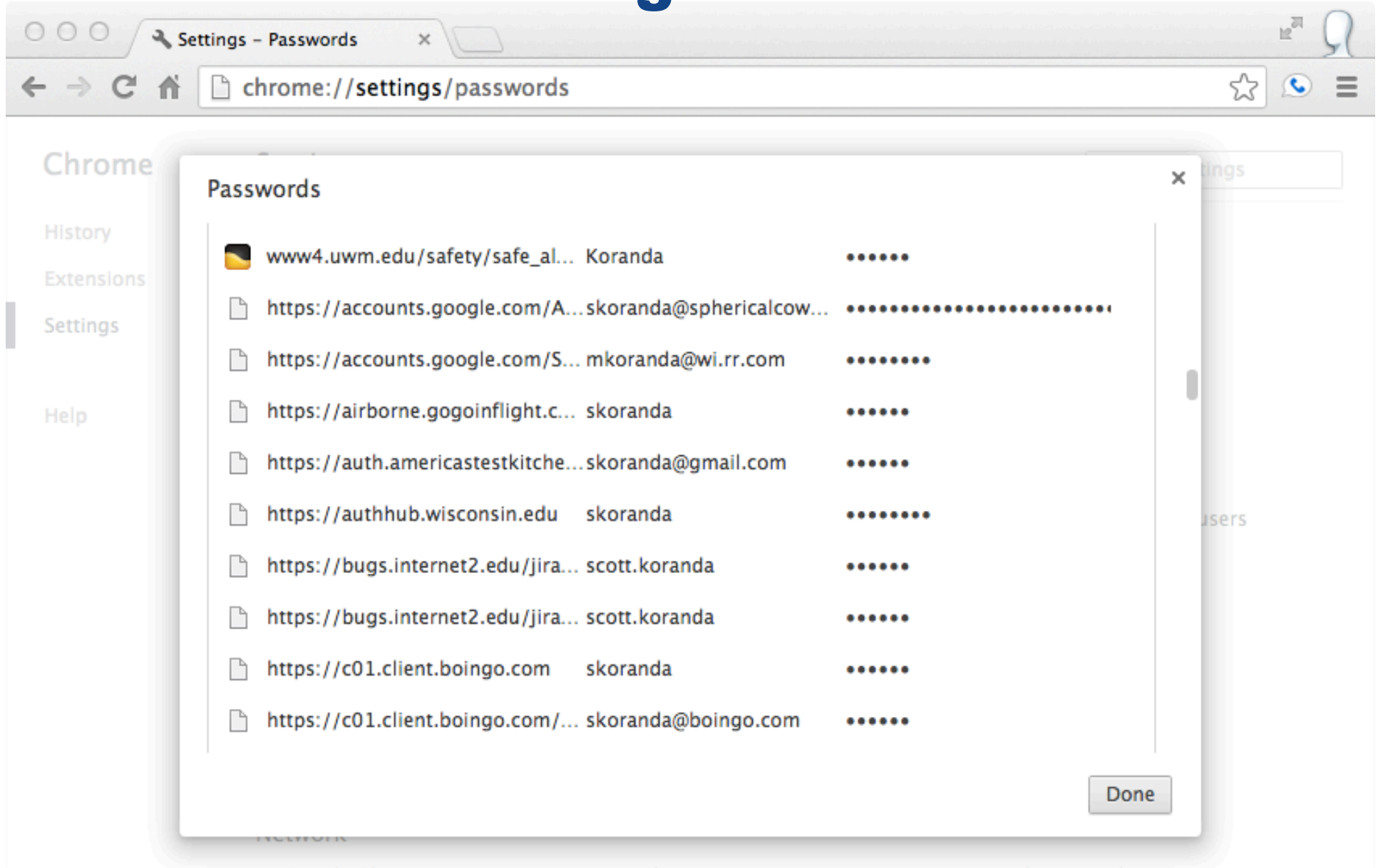
# Federated Versus “Local” Identity

“Local” identity is the identity provisioned for you within a single identity or security domain.

Often the identity provisioned for you by some existing application, service, or tool.

Want to access (login) our project’s resources?  
Create (yet another!) account.

# Ever increasing set of identities



# Federated Identity

Federated identity is an identity you can use across multiple security or identity domains.

Related to, but not the same as, single sign-on (SSO).

SSO provides authentication within a single identity domain (fuzzier for VOs).

# Federated Identity


Might have see already with newer web 2.0 apps.


“Login with your Google/Facebook/Twitter account”

Pinterest

https://www.pinterest.com/login/

## Log in to Pinterest

 Login with Facebook

 Login with Twitter

Email Required

Password

Are you a business? [Get started here](#)

[Forgot your password?](#) [Sign up now](#) [Log in](#)

CTSC

14GO

# Higher Ed & Research Identities

Identity Provider Selection

https://spaces.internet2.edu/shibboleth-ds/WAYF?entityID=https%3A%2F%2Fspaces.inte...

## Select an Identity Provider

The Internet2 Wiki Service requires that you identity yourself. Please select a trusted identity provider from the list below, or simply begin typing in the edit box.

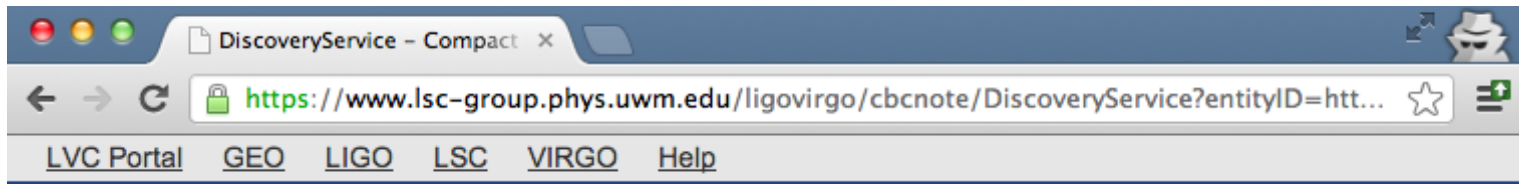
**Enter institution name:**

**Or choose from a list:**

Federation	organization
US Higher Education	Brown University
UK Federation	Bucknell University
SWAMID Test Federation	California Institute of Technology
Austria - ACONet	California Maritime Academy
France - CRU	California Polytechnic State University-San Luis Obispo
Servicio de Identidad de RedIRIS (SIR)	California State Polytechnic University, Pomona
Switzerland - SWITCHaai	California State University, Bakersfield
All Sites	California State University, Channel Islands
	California State University, Chico
	California State University, Dominguez Hills

Need assistance? Send mail to [spaces-admin@internet2.edu](mailto:spaces-admin@internet2.edu) with description.


# LIGO Leverages Federated Identity




[Refresh my LIGO group memberships](#)

## Choose how to login

Use a suggested selection:

  
LIGO

  
LIGO Guest

Or select your organization from the list below

✓ Please select your organization...

LIGO

LIGO Guest

Massachusetts Institute of Technology

Penn State

University of Wisconsin-Milwaukee

[Help](#)

### Navigation

InspiralAnalysisGlossary

RecentChanges

FindPage

HelpContents

DiscoveryService

### Page

Immutable Page

Info

Attachments

### User

Login

[MoinMoin Powered](#)  
[Python Powered](#)  
[GPL licensed](#)  
[Valid HTML 4.01](#)



# Federated Identity

## Pros:

- Users do not have to create new account.
  - “Yet another new account”
- Faster for users to access resource.
- Easier for users to access resource.
- Single credential often protected better.
  - Only one account to manage so manage it well!

# Federated Identity

## Cons:

- New experience for users.
- More mouse clicks just to login to service.
- More complexity for service and infrastructure.
- Error handling more difficult to provide.
- Single credential when compromised is disaster.
  - Bad actors have access across multiple security domains instead of just one.

# Federated Identity: LIGO Use Cases

Consume federated identity and get out of business of providing identity.

- Save substantial help desk support effort.
- Save substantial infrastructure support effort.

Goal, but will be long time coming.

- Need excellent command line support.
- Need sufficient levels of assurance from remote IdPs.
- Need to access identities from around the world.

# Federated Identity: LIGO Use Cases

Streamline collaboration with partners.

- KAGRA (Japan)
- Virgo (French/Italian)
- LIGO-India

Prevent members in each collaboration from having to request and manage identities and credentials provisioned by other collaborations.

# Federated Identity: LIGO Use Cases

Streamline collaboration with astronomers, astrophysicists, and other scientists.

Share, when appropriate, access to analysis results, data, and other scientific work product with colleagues.

# Federated Identity: LIGO Use Cases

Ease processes for review committees, funding agency representatives, and other VIPs.

Prevent VIPs from having to create a LIGO identity or account just to participate on a review panel.

# Trust and Federated Identity

*“All the world is made of faith, and trust, and pixie dust.”*

J. M. Barrie, Peter Pan

# Trust and Federated Identity

How do I know I can trust a remote IdP?

How does the remote IdP know it can trust the SP?

- Doesn't want to allow any service to use it for authenticating users.

Substantially harder when IdP and SP not part of the same organization or security domain.



# Trust the Hard Way

Each IdP, SP negotiates trust in a point-to-point model:

- What identifier is exchanged?
- How information is encrypted and signed?
- Which attributes are asserted?
- How attributes are asserted?
- How attributes are consumed?
- Which privacy policies are in effect?

Legal and policy ramifications cannot be ignored, even for science projects.

## **Need Scalable Trust Model**

Framework for IdPs and SPs to agree to common policies and operating procedures in order to bootstrap trust efficiently across the participants.

IdPs and SPs using SAML as web Authz framework rely on SAML Identity Federations.

# SAML Identity Federation

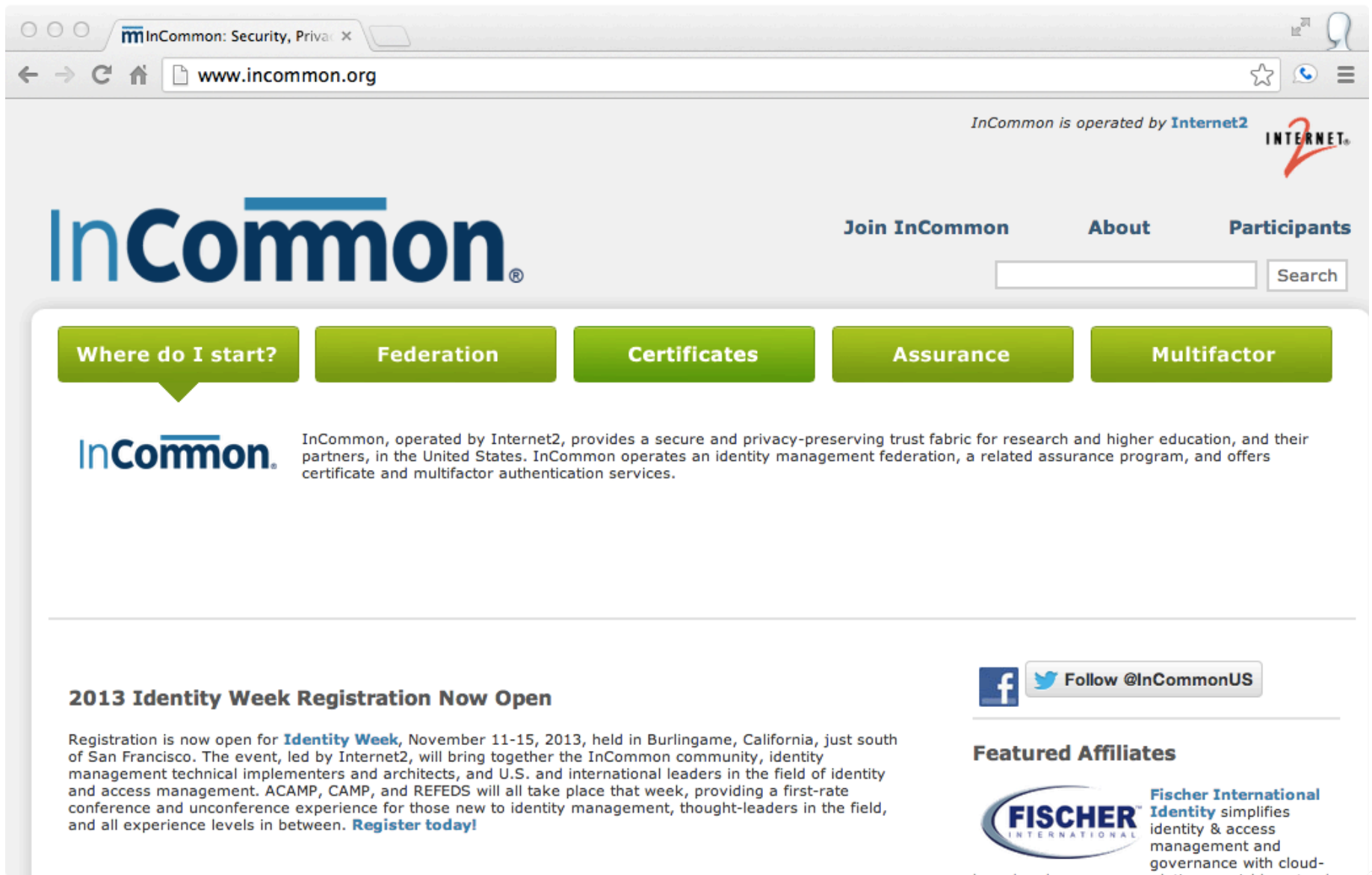
IdP and SP participants agree on:

- Policies for operating IdPs and SPs.
- Establishing trust through exchange of SAML metadata.
  - Details about each IdP and SP, their service endpoints, and how assertions will be signed and encrypted.
- Policies for how metadata is managed.

# SAML Identity Federations

Most SAML identity federations established and operated by national research and education network (NREN) providers.

# US SAML Identity Federation



The screenshot shows the InCommon website in a web browser. The browser's address bar displays 'www.incommon.org'. The page header includes the InCommon logo, navigation links for 'Join InCommon', 'About', and 'Participants', and a search bar. Below the header is a row of five green buttons: 'Where do I start?', 'Federation', 'Certificates', 'Assurance', and 'Multifactor'. The main content area features the InCommon logo and a paragraph describing the organization's mission. A section titled '2013 Identity Week Registration Now Open' provides details about an upcoming event. On the right side, there are social media links for Facebook and Twitter, and a section for 'Featured Affiliates' featuring Fischer International.

InCommon: Security, Privacy

www.incommon.org

InCommon is operated by Internet2

**InCommon**

Join InCommon About Participants

Search

Where do I start? Federation Certificates Assurance Multifactor

**InCommon** InCommon, operated by Internet2, provides a secure and privacy-preserving trust fabric for research and higher education, and their partners, in the United States. InCommon operates an identity management federation, a related assurance program, and offers certificate and multifactor authentication services.

**2013 Identity Week Registration Now Open**

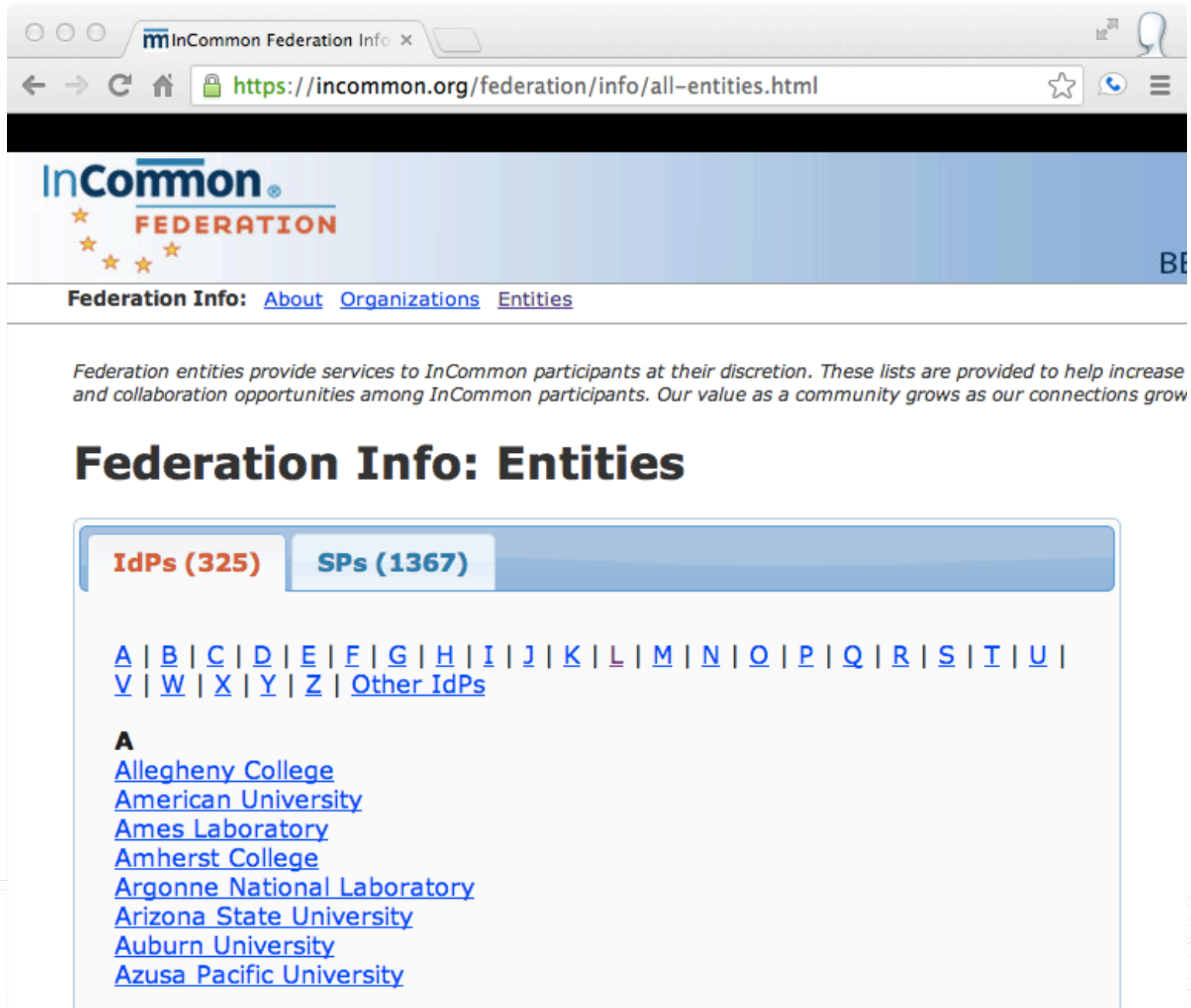
Registration is now open for **Identity Week**, November 11-15, 2013, held in Burlingame, California, just south of San Francisco. The event, led by Internet2, will bring together the InCommon community, identity management technical implementers and architects, and U.S. and international leaders in the field of identity and access management. ACAMP, CAMP, and REFEDS will all take place that week, providing a first-rate conference and unconference experience for those new to identity management, thought-leaders in the field, and all experience levels in between. **Register today!**

**Follow @InCommonUS**

**Featured Affiliates**

**FISCHER** INTERNATIONAL **Fischer International Identity** simplifies identity & access management and governance with cloud-

# 325 IPs and 1367 SPs



The screenshot shows a web browser window with the address bar displaying <https://incommon.org/federation/info/all-entities.html>. The page header features the InCommon Federation logo and navigation links: [Federation Info](#), [About](#), [Organizations](#), and [Entities](#). A paragraph of text states: "Federation entities provide services to InCommon participants at their discretion. These lists are provided to help increase and collaboration opportunities among InCommon participants. Our value as a community grows as our connections grow". The main heading is "Federation Info: Entities". Below this, there are two tabs: "IdPs (325)" and "SPs (1367)". The "IdPs (325)" tab is active. Below the tabs, there is a list of links for each letter of the alphabet (A-Z) and a link for "Other IdPs". The list of IdPs under the letter 'A' includes: [Allegheny College](#), [American University](#), [Ames Laboratory](#), [Amherst College](#), [Argonne National Laboratory](#), [Arizona State University](#), [Auburn University](#), and [Azusa Pacific University](#).

InCommon  
FEDERATION

Federation Info: [About](#) [Organizations](#) [Entities](#)

Federation entities provide services to InCommon participants at their discretion. These lists are provided to help increase and collaboration opportunities among InCommon participants. Our value as a community grows as our connections grow

## Federation Info: Entities

**IdPs (325)** **SPs (1367)**

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#) | [Other IdPs](#)


**A**

- [Allegheny College](#)
- [American University](#)
- [Ames Laboratory](#)
- [Amherst College](#)
- [Argonne National Laboratory](#)
- [Arizona State University](#)
- [Auburn University](#)
- [Azusa Pacific University](#)

# LIGO IdP in InCommon

InCommon Federation Info: x

https://incommon.org/federation/info/all-entities.html#IdPs\_L



---

**Identity Provider:** **LIGO Scientific Collaboration** [more technical info](#)

**Description:** *Laser Interferometer Gravitational-Wave Observatory (LIGO)*

**Information URL:** <https://dcc.ligo.org/cgi-bin/DocDB/ShowDocument?docid=89286>

**Privacy Statement URL:** <https://dcc.ligo.org/cgi-bin/DocDB/ShowDocument?docid=89243>


**Technical Contacts:** "Scott Koranda" <scott.koranda@ligo.org>

**Administrative Contacts:** "Warren Anderson" <warren.anderson@ligo.org>

**Support Contacts:** "LIGO Identity Management Help Desk" <rt-auth@ligo.org>

**Site Administrators:** Visit the wiki for documentation regarding [MDUI elements](#) and [contacts](#) in IdP metadata.

---



This InCommon Identity Provider is owned by:  
[LIGO Scientific Collaboration](#)

Questions? Visit our [FAQ](#) or contact  
<info at incommon dot org>


Mayo Clinic  
McNally Smith College

# LIGO SP in InCommon

InCommon Federation Info x

← → ↻ ⬆ [https://incommon.org/federation/info/all-entities.html#SPs\\_L](https://incommon.org/federation/info/all-entities.html#SPs_L) ☆ 📞 ☰

---



---

**Service Provider:** **LIGO Wiki** [more technical info](#)

**Description:** *Primary LIGO Scientific Collaboration wiki*

**Information URL:** <https://wiki.ligo.org/Main/SPInformationURL>

**Privacy Statement URL:** <https://dcc.ligo.org/cgi-bin/DocDB/ShowDocument?docid=89243>


**Technical Contacts:** "Scott Koranda" <scott.koranda@ligo.org>

**Administrative Contacts:** "Warren Anderson" <warren.anderson@ligo.org>

**Support Contacts:** "LIGO Identity Management Help Desk" <rt-auth@ligo.org>

**Site Administrators:** Visit the wiki for documentation regarding [MDUI elements](#), [requested attributes](#), and [contacts](#) in SP metadata.

---

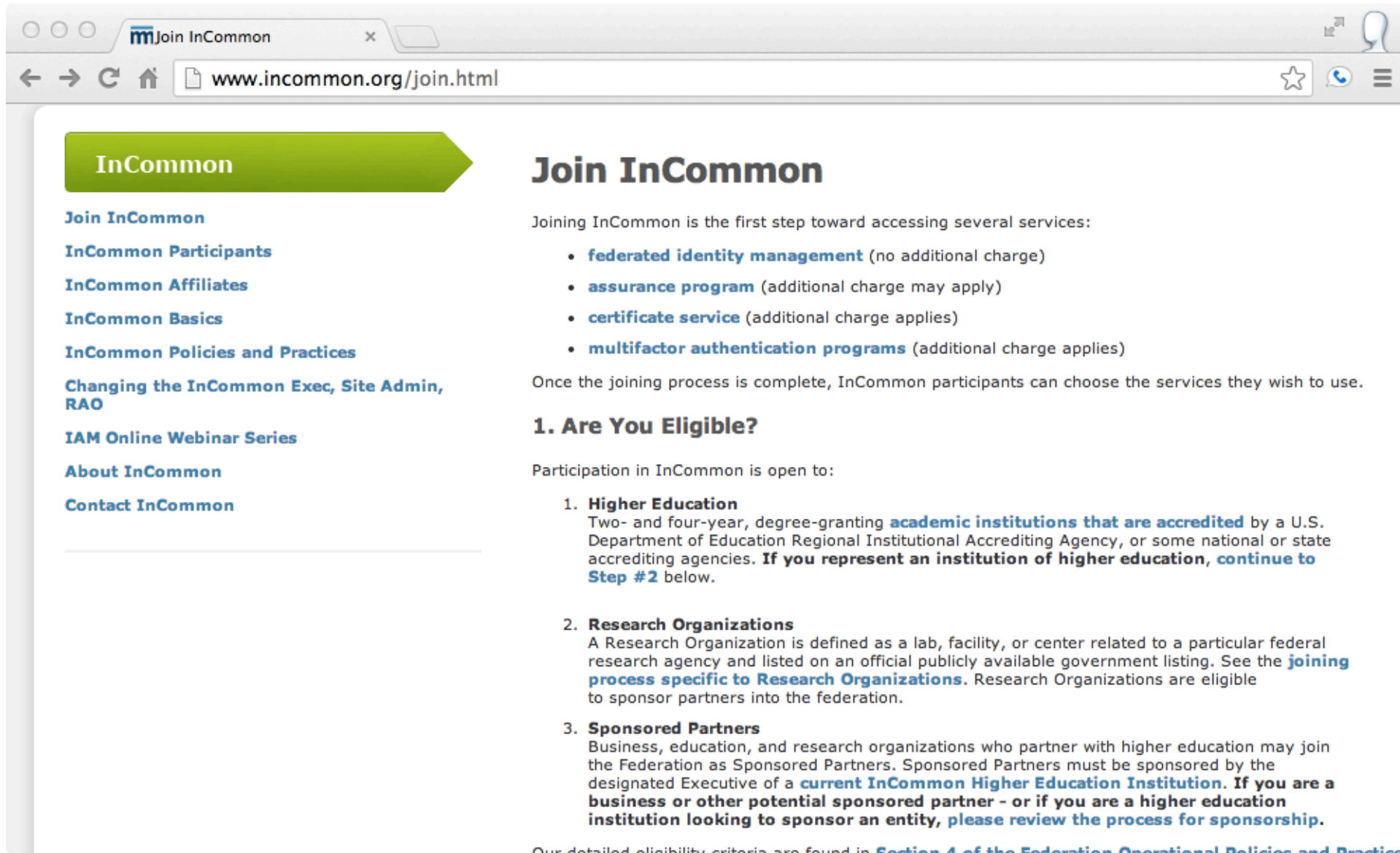


This InCommon registered service is owned by:  
[LIGO Scientific Collaboration](#)

Questions? Visit our [FAQ](#) or contact  
<info at incommon dot org>



# Research VOs May Join



The screenshot shows a web browser window with the address bar displaying [www.incommon.org/join.html](http://www.incommon.org/join.html). The page has a green header with the InCommon logo. On the left is a navigation menu with links: Join InCommon, InCommon Participants, InCommon Affiliates, InCommon Basics, InCommon Policies and Practices, Changing the InCommon Exec, Site Admin, RAO, IAM Online Webinar Series, About InCommon, and Contact InCommon. The main content area is titled 'Join InCommon' and explains that joining is the first step toward accessing several services:

- **federated identity management** (no additional charge)
- **assurance program** (additional charge may apply)
- **certificate service** (additional charge applies)
- **multifactor authentication programs** (additional charge applies)

Once the joining process is complete, InCommon participants can choose the services they wish to use.

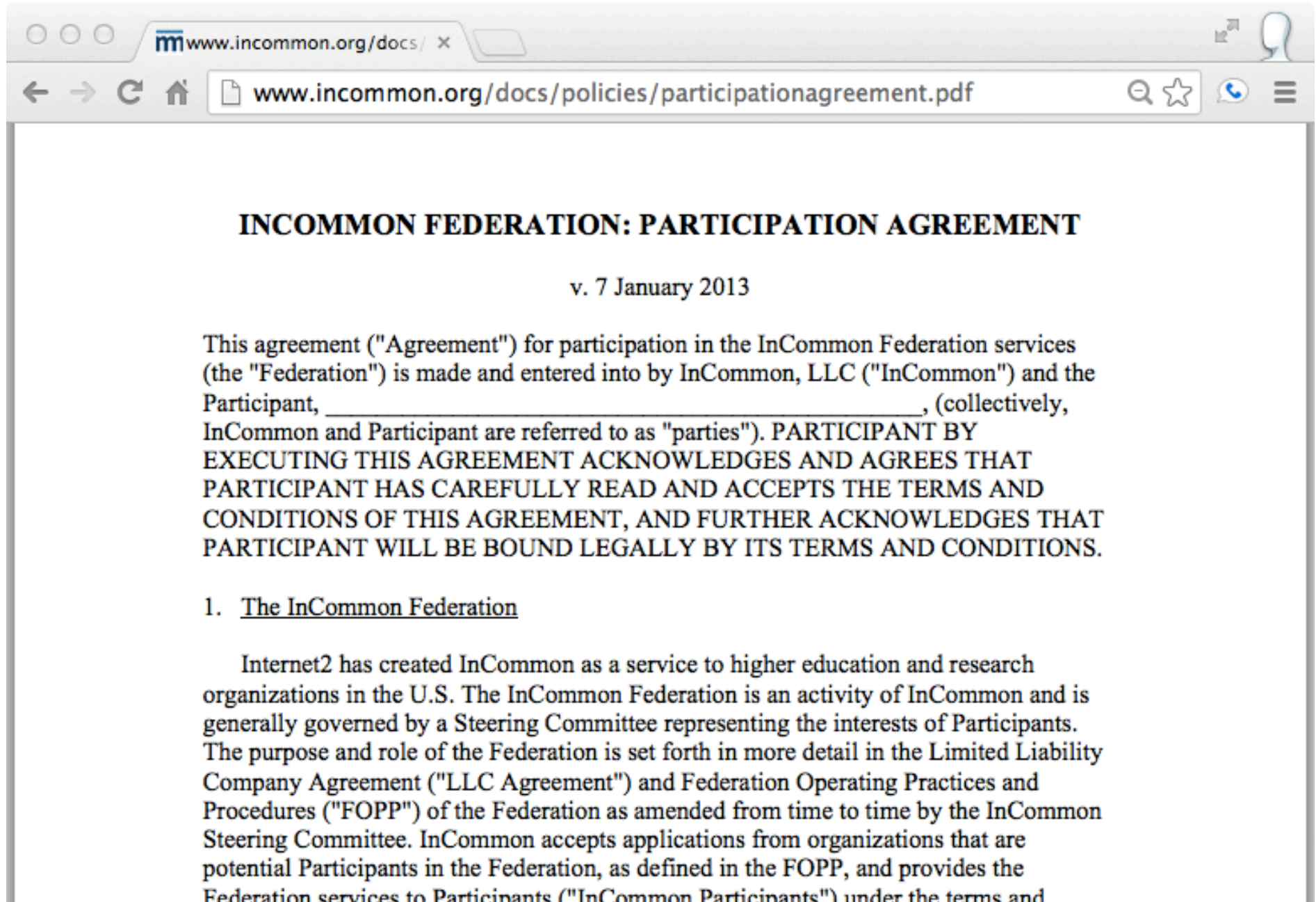
## 1. Are You Eligible?

Participation in InCommon is open to:

- 1. Higher Education**  
Two- and four-year, degree-granting **academic institutions that are accredited** by a U.S. Department of Education Regional Institutional Accrediting Agency, or some national or state accrediting agencies. **If you represent an institution of higher education, continue to Step #2** below.
- 2. Research Organizations**  
A Research Organization is defined as a lab, facility, or center related to a particular federal research agency and listed on an official publicly available government listing. See the **joining process specific to Research Organizations**. Research Organizations are eligible to sponsor partners into the federation.
- 3. Sponsored Partners**  
Business, education, and research organizations who partner with higher education may join the Federation as Sponsored Partners. Sponsored Partners must be sponsored by the designated Executive of a **current InCommon Higher Education Institution**. **If you are a business or other potential sponsored partner - or if you are a higher education institution looking to sponsor an entity, please review the process for sponsorship.**

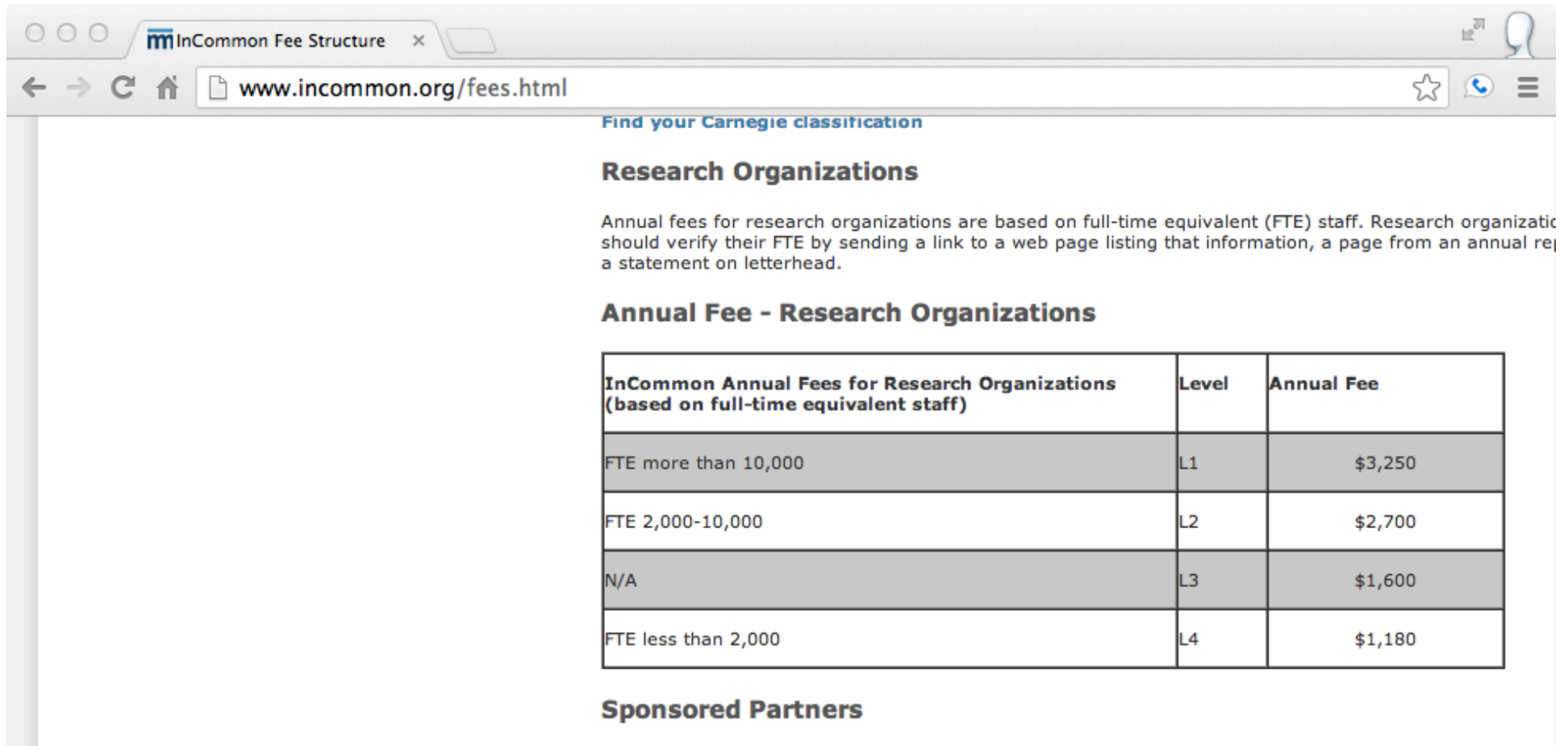
Our detailed eligibility criteria are found in **Section 4 of the Federation Operational Policies and Practices**.

# VOs Sign Participant Agreement



The image is a screenshot of a web browser window. The address bar shows the URL [www.incommon.org/docs/policies/participationagreement.pdf](http://www.incommon.org/docs/policies/participationagreement.pdf). The page content is a PDF document titled "INCOMMON FEDERATION: PARTICIPATION AGREEMENT" with a version date of "v. 7 January 2013". The text of the agreement begins with "This agreement ('Agreement') for participation in the InCommon Federation services (the 'Federation') is made and entered into by InCommon, LLC ('InCommon') and the Participant, \_\_\_\_\_, (collectively, InCommon and Participant are referred to as 'parties'). PARTICIPANT BY EXECUTING THIS AGREEMENT ACKNOWLEDGES AND AGREES THAT PARTICIPANT HAS CAREFULLY READ AND ACCEPTS THE TERMS AND CONDITIONS OF THIS AGREEMENT, AND FURTHER ACKNOWLEDGES THAT PARTICIPANT WILL BE BOUND LEGALLY BY ITS TERMS AND CONDITIONS." The first section is titled "1. The InCommon Federation". The text under this section states: "Internet2 has created InCommon as a service to higher education and research organizations in the U.S. The InCommon Federation is an activity of InCommon and is generally governed by a Steering Committee representing the interests of Participants. The purpose and role of the Federation is set forth in more detail in the Limited Liability Company Agreement ('LLC Agreement') and Federation Operating Practices and Procedures ('FOPP') of the Federation as amended from time to time by the InCommon Steering Committee. InCommon accepts applications from organizations that are potential Participants in the Federation, as defined in the FOPP, and provides the Federation services to Participants ('InCommon Participants') under the terms and

# VOs pay \$ to InCommon



The screenshot shows a web browser window with the address bar displaying [www.incommon.org/fees.html](http://www.incommon.org/fees.html). The page title is "InCommon Fee Structure". The main content area has a heading "Find your Carnegie classification" and a subheading "Research Organizations". Below this, a paragraph states: "Annual fees for research organizations are based on full-time equivalent (FTE) staff. Research organizations should verify their FTE by sending a link to a web page listing that information, a page from an annual report, or a statement on letterhead." This is followed by a subheading "Annual Fee - Research Organizations" and a table with three columns: "InCommon Annual Fees for Research Organizations (based on full-time equivalent staff)", "Level", and "Annual Fee". The table contains four rows of data. Below the table is a subheading "Sponsored Partners".

**Research Organizations**

Annual fees for research organizations are based on full-time equivalent (FTE) staff. Research organizations should verify their FTE by sending a link to a web page listing that information, a page from an annual report, or a statement on letterhead.

**Annual Fee - Research Organizations**

InCommon Annual Fees for Research Organizations (based on full-time equivalent staff)	Level	Annual Fee
FTE more than 10,000	L1	\$3,250
FTE 2,000-10,000	L2	\$2,700
N/A	L3	\$1,600
FTE less than 2,000	L4	\$1,180

**Sponsored Partners**

# Challenges Joining InCommon

Many VOs not legal entities.

- LIGO is not a legal entity.
- Caltech signed on behalf of LIGO.
  - Includes people not on Caltech campus.
  - Why should Caltech assume that risk?
- InCommon needs to broaden interpretation of sharing risk.
  - Indemnification and insurance not only way to mitigate risk.
  - Need better models for distributed research VOs.
- VOs should leverage willing campus sponsors.

# Challenges Joining InCommon

Culture based on campuses and not VOs.

- Changing but still an issue at times.
- Different balance between risk and rewards.
- Different timescale than many VOs.
  - 3 years for major initiative not uncommon.
  - A research VO may come and go in 3 years.
  - Positive is long term stability.

# Joining InCommon

Joining InCommon is a legal agreement.

Does not require technical infrastructure so can begin joining process early before ready for consuming federated identity.

# Leveraging InCommon

Register SP to consume federated identities.

- Publish SP metadata into InCommon feed.
- Feed consumed by InCommon IdPs.
- Enables interoperability between SP and IdPs.

Step 0: deploy Shibboleth SP

- Use your best web application people.

# Publish SP into InCommon

new\_sp : LIGO Scientific Co x

← → ↻ ⌂ [https://service1.internet2.edu/siteadmin/10386/new\\_sp](https://service1.internet2.edu/siteadmin/10386/new_sp) ☆ ☎ ☰

## InCommon Site Admin: LIGO Scientific Collaboration

scott.koranda@ligo.org ([Logout](#))

- Home
- x.509 Certificates (IdP only)
- Identity Provider Metadata Wizard
- Service Provider Metadata Wizard
- Delegated Administrators
- POPs
- Your Account
- Documentation
- FM Change Log

### New Service Provider

\* Denotes a required field

**Input your host name and choose your server software to automatically fill out this form, or specify values manually.**

Hostname:  SP Server Software:

OR

EntityID\*: (example, "https://service.example.org/shibboleth", [more...](#))

#### User Interface Elements and Requested Attributes: \*

User Interface Elements: ([Help](#))

\* SP Display Name:

SP Description:

SP Information URL:

SP Privacy Statement URL:

SP Logo HTTPS URL:

SP Logo Width x Height:  x  (pixels)

Requested Attributes: ([Help](#))

Attribute Name:



# **Publish SP in InCommon**

Sounds great!

- Deploy Shibboleth on your web server.
- Publish SP into InCommon metadata.
- Consume federated identities from 300+ IdPs.
- Never issue a password again!

What's the catch?

# Publishing SP **Enables** Interoperability

Does **NOT** guarantee interoperability.

- IdPs free to ignore your SP and some will.
  - A few “well known” campuses do not collaborate by default.
- Does your application need anything more than authentication?
  - Default for many IdPs is binary yes/no of authentication event.

## InCommon IdPs

Most IdPs send opaque, targeted, transient identifier and nothing else.

<saml2:NameID

Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"

NameQualifier="https://login.ligo.org/idp/shibboleth"

SPNameQualifier="https://wiki.ligo.org/shibboleth-sp"

>\_708b4a90108f5cb2a424534495ffd081</saml2:NameID>

Driven by privacy concerns (FERPA anyone?)

Yes, given name, sn, email considered private.

# InCommon IdPs

*"Who are you?"*

*"No one of consequence."*

*"I must know."*

*"Get used to disappointment."*

William Goldman, *The Princess Bride*

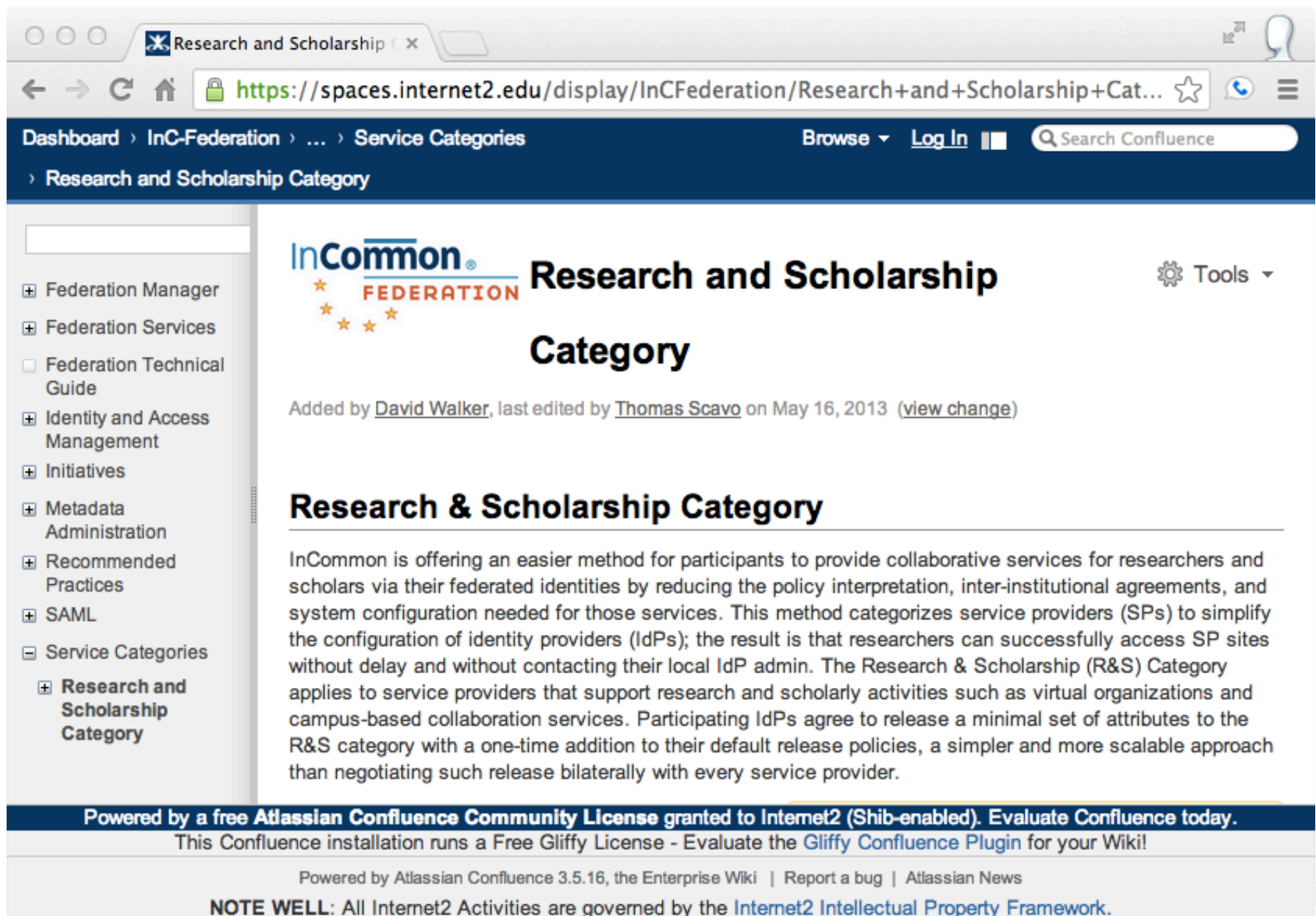
# Applications Need More Attributes

Most VO web applications require more from a federated identity:

- given name
- family name
- email
- non-transient or persistent
- non-targeted or same for all SPs
- non-opaque since often “seen” by humans

This default for most InCommon IdPs is a serious limitation for science VOs.

# InCommon R&S Category



The screenshot shows a web browser window displaying the InCommon Research and Scholarship Category page. The browser's address bar shows the URL <https://spaces.internet2.edu/display/InCFederation/Research+and+Scholarship+Cat...>. The page has a dark blue header with navigation links: [Dashboard](#) > [InC-Federation](#) > ... > [Service Categories](#). On the right of the header are links for [Browse](#), [Log In](#), and a [Search Confluence](#) bar. Below the header, the page title is **Research and Scholarship Category**. The main content area features the InCommon Federation logo, the title **Research and Scholarship Category**, and a note: *Added by [David Walker](#), last edited by [Thomas Scavo](#) on May 16, 2013 ([view change](#))*. The left sidebar contains a list of navigation items: Federation Manager, Federation Services, Federation Technical Guide, Identity and Access Management, Initiatives, Metadata Administration, Recommended Practices, SAML, Service Categories, and **Research and Scholarship Category**. The main text describes the category's purpose: "InCommon is offering an easier method for participants to provide collaborative services for researchers and scholars via their federated identities by reducing the policy interpretation, inter-institutional agreements, and system configuration needed for those services. This method categorizes service providers (SPs) to simplify the configuration of identity providers (IdPs); the result is that researchers can successfully access SP sites without delay and without contacting their local IdP admin. The Research & Scholarship (R&S) Category applies to service providers that support research and scholarly activities such as virtual organizations and campus-based collaboration services. Participating IdPs agree to release a minimal set of attributes to the R&S category with a one-time addition to their default release policies, a simpler and more scalable approach than negotiating such release bilaterally with every service provider."

Powered by a free **Atlassian Confluence Community License** granted to Internet2 (Shib-enabled). Evaluate Confluence today.  
This Confluence installation runs a Free Gliffy License - Evaluate the [Gliffy Confluence Plugin](#) for your Wiki!

Powered by Atlassian Confluence 3.5.16, the Enterprise Wiki | [Report a bug](#) | [Atlassian News](#)

**NOTE WELL:** All Internet2 Activities are governed by the [Internet2 Intellectual Property Framework](#).

# R&S Tags in InCommon Metadata

```
<EntityDescriptor entityID="https://wiki.ligo.org/shibboleth-sp">
```

```
<Extensions>
```

```
<mdattr:EntityAttributes>
```

```
<saml:Attribute>
```

```
<saml:AttributeValue>
```

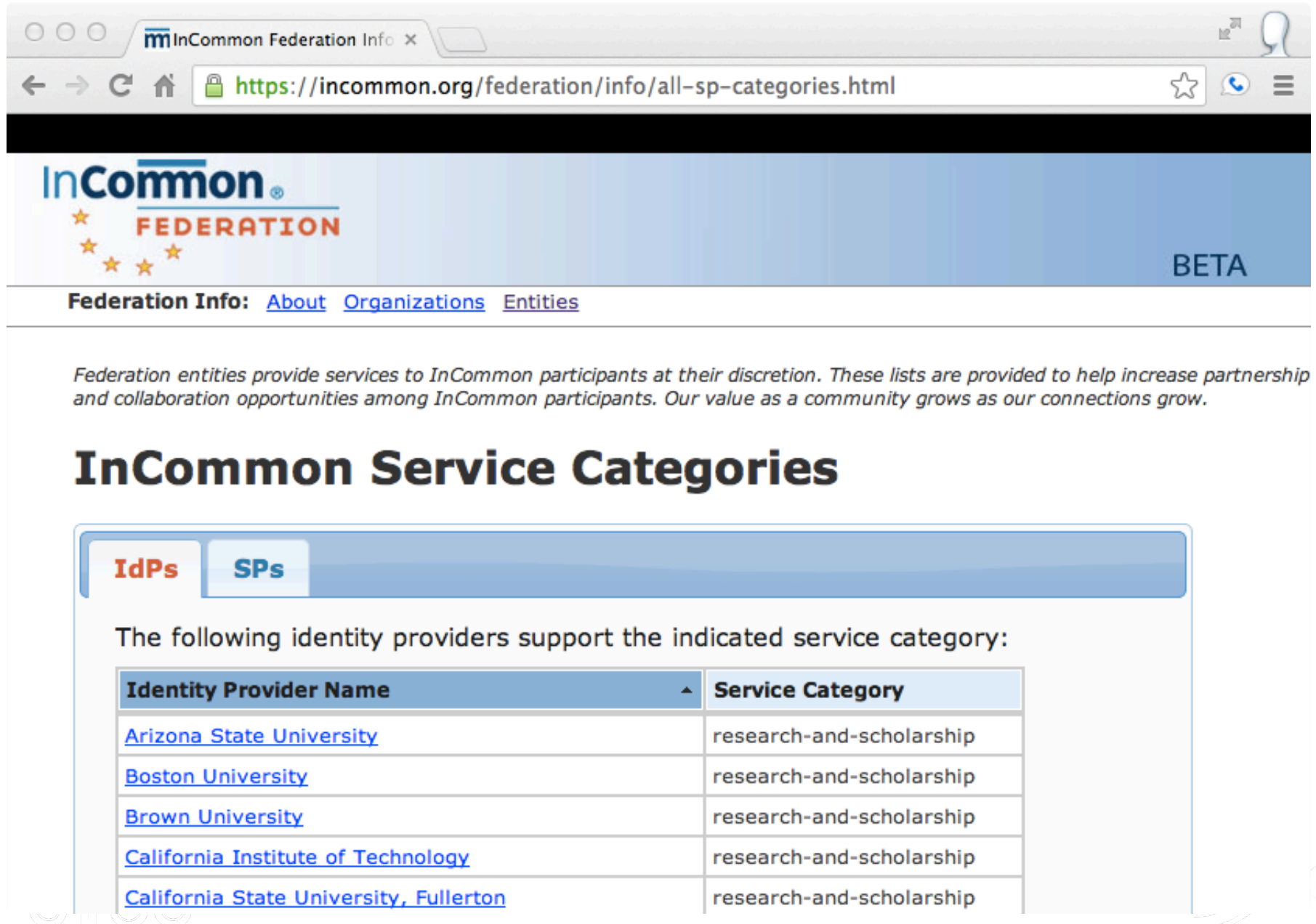
```
http://id.incommon.org/category/research-and-scholarship
```

```
</saml:AttributeValue>
```

```
</saml:Attribute>
```

```
</mdattr:EntityAttributes>
```

# 58 InCommon IdPs



The screenshot shows a web browser window with the address bar displaying <https://incommon.org/federation/info/all-sp-categories.html>. The page header features the InCommon Federation logo and a 'BETA' label. Below the header, there are navigation links for 'About', 'Organizations', and 'Entities'. A paragraph of text explains the purpose of the federation entities. The main section is titled 'InCommon Service Categories' and contains two tabs: 'IdPs' (selected) and 'SPs'. Under the 'IdPs' tab, a message states: 'The following identity providers support the indicated service category:'. Below this message is a table with two columns: 'Identity Provider Name' and 'Service Category'. The table lists five identity providers, all of which support the 'research-and-scholarship' service category.

**InCommon**  
FEDERATION

BETA

Federation Info: [About](#) [Organizations](#) [Entities](#)

*Federation entities provide services to InCommon participants at their discretion. These lists are provided to help increase partnership and collaboration opportunities among InCommon participants. Our value as a community grows as our connections grow.*

## InCommon Service Categories

**IdPs** **SPs**

The following identity providers support the indicated service category:

Identity Provider Name	Service Category
<a href="#">Arizona State University</a>	research-and-scholarship
<a href="#">Boston University</a>	research-and-scholarship
<a href="#">Brown University</a>	research-and-scholarship
<a href="#">California Institute of Technology</a>	research-and-scholarship
<a href="#">California State University, Fullerton</a>	research-and-scholarship



## InCommon R&S

“InCommon IdPs are strongly encouraged to release the following attributes to R&S category SPs:

- personal identifiers: email address, person name, eduPersonPrincipalName
- pseudonymous identifier: eduPersonTargetedID
- affiliation: eduPersonScopedAffiliation

where email address refers to the mail attribute and person name refers to displayName and optionally givenName and sn (i.e., surName).”

# InCommon R&S

R&S Service Providers must comply with the following requirements:

- The service enhances the research and scholarship activities of some subset of the InCommon community.
- The service meets the following technical requirements:
  - Service metadata has been submitted to InCommon and published in a human-readable format on the InCommon public web site.
  - The SP is a production SAML deployment that supports SAML V2.0 Web Browser SSO.
  - The SP refreshes and verifies metadata at least daily.
  - The SP provides an mdui:DisplayName in metadata (one of numerous User Interface Elements).
  - The SP supports the SAML V2.0 HTTP-POST binding (one of numerous SAML V2.0 endpoints in metadata)
  - The SP provides Technical and Administrative contacts in metadata.
  - The SP provides requested attributes in metadata.

# InCommon Assurance

*“I can assure you, my intentions are strictly honorable.”*

James Bond, Dr. No

# InCommon Trust

All participants required to publish POP.

- Participant Operational Practices.
- Details
  - Electronic identity credentials.
  - Electronic identity database.
  - Attribute Assertions.
  - Privacy Policy.
  - Technical standards.
- Available for inspection by other participants.

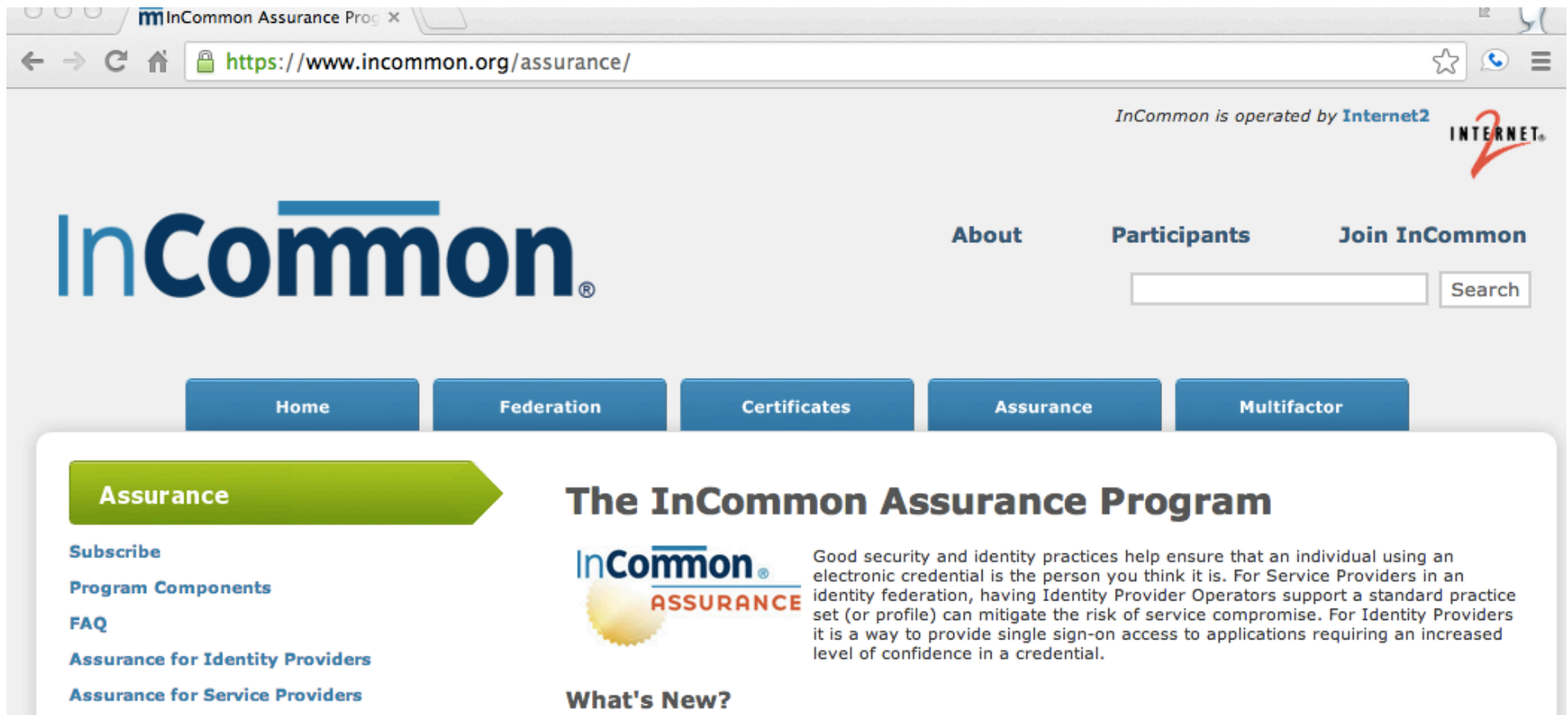
## InCommon POP

POP good idea but failed implementation:

- Not all participants have filed a POP.
- Many are > 5 years out of date.
- No framework so level of detail varies.

Hard to measure risk for entire trust fabric based on the current collection of POPs.

# InCommon Assurance Program



The screenshot shows the InCommon Assurance Program website. The browser address bar displays <https://www.incommon.org/assurance/>. The page header includes the InCommon logo, navigation links for "About", "Participants", and "Join InCommon", and a search bar. A secondary navigation bar contains links for "Home", "Federation", "Certificates", "Assurance", and "Multifactor". The main content area features a green arrow pointing to the "Assurance" section, which includes links for "Subscribe", "Program Components", "FAQ", "Assurance for Identity Providers", and "Assurance for Service Providers". The "The InCommon Assurance Program" section explains the program's purpose: "Good security and identity practices help ensure that an individual using an electronic credential is the person you think it is. For Service Providers in an identity federation, having Identity Provider Operators support a standard practice set (or profile) can mitigate the risk of service compromise. For Identity Providers it is a way to provide single sign-on access to applications requiring an increased level of confidence in a credential." Below this is a "What's New?" section.

InCommon Assurance Program

InCommon is operated by Internet2

**InCommon**

About Participants Join InCommon

Search

Home Federation Certificates Assurance Multifactor

**Assurance**

Subscribe

Program Components

FAQ

Assurance for Identity Providers

Assurance for Service Providers

## The InCommon Assurance Program

**InCommon**  
ASSURANCE

Good security and identity practices help ensure that an individual using an electronic credential is the person you think it is. For Service Providers in an identity federation, having Identity Provider Operators support a standard practice set (or profile) can mitigate the risk of service compromise. For Identity Providers it is a way to provide single sign-on access to applications requiring an increased level of confidence in a credential.

What's New?

# InCommon Assurance

- Identity Assurance Profiles.
  - IdP operator requirements for registration, credential issuance, technical operations.
  - Bronze and Silver Profiles.
  - Bronze with or without audit, Silver requires audit.
- Identity Assurance Assessment Framework.
  - Background on need for assurance.
  - Defines trust model.
  - Functional model for IdPs.
  - Certification model.
- Informed by but NOT NIST 800-63.
- By Higher Ed and Research for Higher Ed and Research.

# InCommon Assurance

- Alternative means.
  - Allows IdPs to petition for alternative mechanism for meeting profile requirements.
  - Intended to provide necessary flexibility.
- Assurance Advisory Committee.
  - Program oversight by community.
  - Reports to steering.
  - Representation by SPs.
  - LIGO representation through 2013.
  - Need more VOs to step up!



# InCommon Assurance

## Benefits of Assurance

- Increases confidence, reduces risk.
- Getting past passwords—community standards until they are gone.
- It's not NIST 800-63. It's Higher Ed's version.
- Saves time when adding new partners.
- Access to Higher-Value Services like financial and health related.
- Protects your investment — InCommon is an approved Trust Framework Provider under the U.S. Identity, Credential, and Access Management Trust Framework Program.

# InCommon Assurance

Substantial investment by InCommon and group of thought leaders.

- Great deal of work by community leaders.
- Well designed and executed so far.

# InCommon Assurance

To date one (1) IdP asserts Silver (and Bronze).

- Virginia Tech
- Used alternative means with 2-factor auth.

Slow uptake so far.

- Real costs for campus IdP operators.
  - Staff time.
  - Audit time.
- SP consumers have not arrived.
  - Science VOs could have big impact here.



# Beyond InCommon

*“You may say I'm a dreamer, but I'm not the only one. I hope someday you'll join us, and the world will be as one.”*

John Lennon, Imagine

# Beyond InCommon

InCommon gives an SP access to > 300 US IdPs

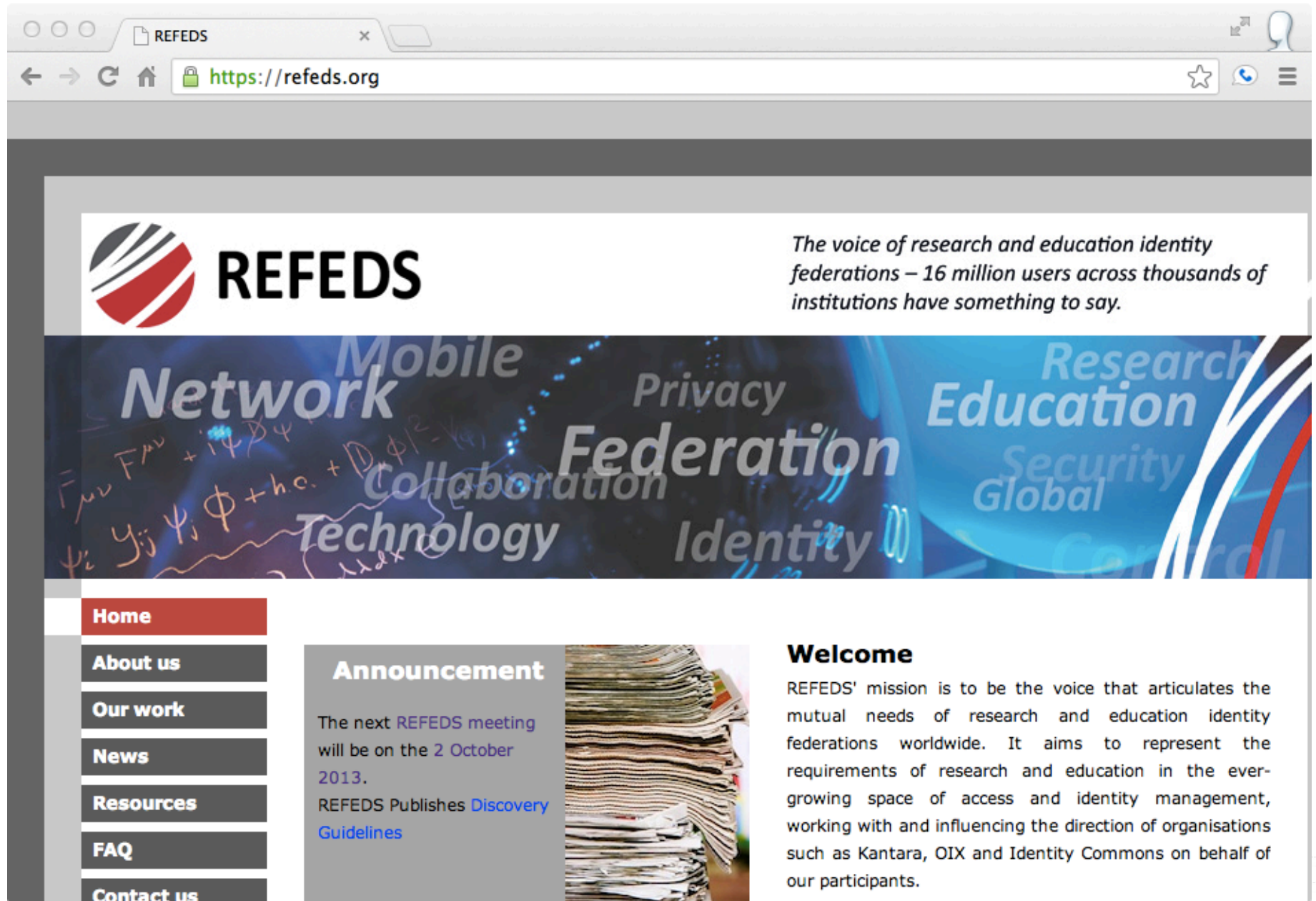
What of the world beyond?

## Other SAML Identity Federations

Most European countries, Canada, and Japan have well established SAML identity federations with high coverage in academia and research.

Federations in China, South America, Latin America, and India either newly formed or coming online soon.

# REFEDS



The screenshot shows a web browser window with the address bar displaying <https://refeds.org>. The website header features the REFEDS logo, which consists of a stylized red and black circle, followed by the word "REFEDS" in bold black text. To the right of the logo, a tagline reads: "The voice of research and education identity federations – 16 million users across thousands of institutions have something to say."

Below the header is a large banner image with a blue and black background. It contains several words in a stylized font: "Network", "Mobile", "Privacy", "Research", "Education", "Security", "Global", "Federation", "Collaboration", "Technology", and "Identity". There are also some mathematical symbols and formulas scattered across the banner.

On the left side of the page, there is a vertical navigation menu with the following items: "Home" (highlighted in red), "About us", "Our work", "News", "Resources", "FAQ", and "Contact us".

The main content area is divided into two columns. The left column has a section titled "Announcement" with the text: "The next REFEDS meeting will be on the 2 October 2013. REFEDS Publishes [Discovery Guidelines](#)". To the right of this text is a small image of a stack of papers. The right column has a section titled "Welcome" with the text: "REFEDS' mission is to be the voice that articulates the mutual needs of research and education identity federations worldwide. It aims to represent the requirements of research and education in the ever-growing space of access and identity management, working with and influencing the direction of organisations such as Kantara, OIX and Identity Commons on behalf of our participants."

# REFEDS

“The mission of REFEDS is to be the voice that articulates the mutual needs of research and education identity federations worldwide. The group represents the requirements of research and education in the ever-growing space of access and identity management...”



Federations - REFEDs

<https://refeds.terena.org/index.php/Federations>

- Cite this page
- Print as PDF

CA	Canadian Access Federation CAF
CH	SWITCHaai
CL	COFRE
CN	CARSI
CZ	eduID.cz
DE	DFN-AAI
DK	WAYF
EE	TAAT
ES	SIR
FI	Haka
FR	Fédération Éducation-Recherche
GR	GRNET
HR	AAI@EduHr
HU	eduID.hu (HREF Federation)
IE	EduGate
IN	INFLIBNET Access Management Federation
IT	IDEM
JP	GakuNin
LV	LAIFE
MY	MyIFAM
NL	SURFnet
NO	FEIDE

# International Federation

How does a VO interoperate with international relying parties (IdPs or SPs)?

# International Federation

Three (3) basic approaches:

1. Point-to-point: negotiate each IdP/SP.
2. Join each relevant national federation.
3. Leverage existing InCommon investment.
  - InCommon pursuing bilateral agreements.
  - InCommon pursuing eduGAIN.

## Point-to-point federation

- Usually fastest means to an end.
- Helpful to understand technical challenges.
- Not always an option for IdPs.
- Clearly does not scale.

## Joining other Federations

- Spectrum of agreement frameworks varies.
- Some require legal documents.
- Fees vary for VOs.
- Privacy laws further complicate issue.
- Best if targeted at narrow group of IdPs/SPs.

# InCommon and Interfederation

InCommon pursuing first bilateral agreement.

- UK Access Federation.
- Large and comprehensive coverage of UK.
- Platform for exploring complicated issues.
  - Are all entities exchanged or some subset?
  - Can there be agreement on attribute release?
  - Can there be agreement on assurance?
- Led by InCommon Interfederation Working Group
  - Chartered by InCommon Technical Advisory Committee.

# eduGAIN

AbouteduGAIN

www.geant.net/service/eduGAIN/about\_edugain/Pages/AbouteduGAIN.aspx

FAQs | CONTACT US | SITEMAP | COOKIE POLICY | GÉANT GATEWAY

GÉANT

ABOUT GÉANT | NETWORK | INNOVATION | SERVICES | USERS | NEWS & EVENTS | RESOURCES

GÉANT > service > eduGAIN > About eduGAIN

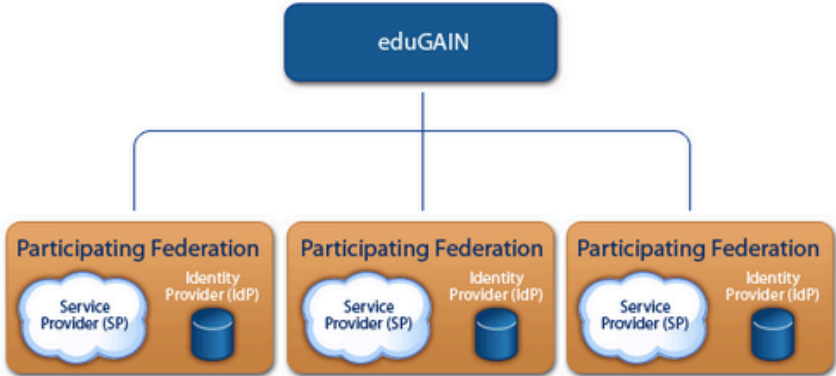
eduGAIN

[About eduGAIN](#)  
[User Experience](#)  
[FAQs](#)  
[Resources](#)  
[Technical Information](#)  
[About Us](#)  
[Contact Us](#)

## About eduGAIN

eduGAIN is a service developed within the GÉANT project. eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating elements of the federations' technical infrastructure and providing a policy framework that controls this information exchange.

This exchange of information contributes to the seamless operation of services developed within the GÉANT project and services provided by other communities represented by, or associated with, the GÉANT Partners.



```
graph TD; eduGAIN[eduGAIN] --- F1[Participating Federation]; eduGAIN --- F2[Participating Federation]; eduGAIN --- F3[Participating Federation]; F1 --- SP1((Service Provider SP)); F1 --- IdP1((Identity Provider IdP)); F2 --- SP2((Service Provider SP)); F2 --- IdP2((Identity Provider IdP)); F3 --- SP3((Service Provider SP)); F3 --- IdP3((Identity Provider IdP));
```

Features:

CTS

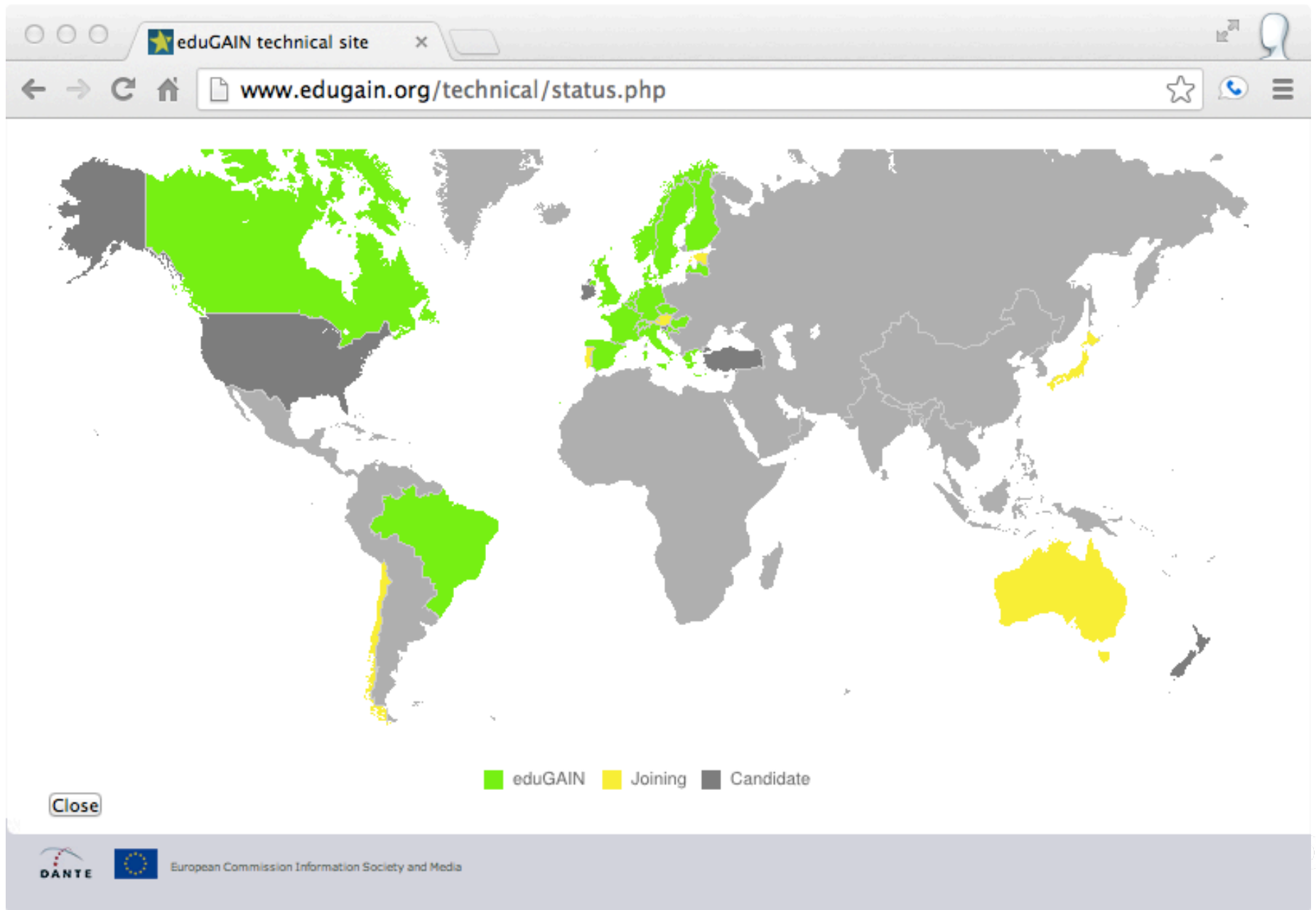
Logo

# eduGAIN

“eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating elements of the federations’ technical infrastructure and providing a policy framework that controls this information exchange.”



**eduGAIN**



# InCommon and eduGAIN

Work underway for InCommon to participate.

- Also led by Interfederation Working Group.
- eduGAIN based on “unilateral declarations”.
- InCommon preparing to declare.
- Possible participation by Q1 2014?

# InCommon and eduGAIN

Participation helps but many issues remain.

- Attribute release.
- Attribute categories (R&S?).
- Levels of Assurance.
- No guarantee IdP a VO needs participate.
- VOs needed to help drive use cases.

# Application Integration Challenges

*“You want answers?”*

*“I think I’m entitled.”*

*“You want answers?!”*

*“I want the truth!”*

*“You can’t handle the truth!”*

A Few Good Men

# Application Integration Challenges

Many apps not ready for federated identity.

- Assume a local store for login & password.
- Mix authentication and authorization.
- Assume email is a perfect identifier.
  - Never changes.
  - Never reassigned.
  - Single domain.
- Assume human consumable identifier.
- Built-in weak and coarse grained authz.
- Retrofit can be a lot of work.

# LIGO “Domestications”

## Done by LIGO

- Foswiki (Twiki)
- Moin
- MediaWiki
- Dokuwiki
- electronic notebook
- document control center
- electronic voting (halo)

## Leveraged by LIGO

- Sympa (email)
- Grouper
- Drupal

# Application Development Tips

- Expect opaque identifier(s).
  - Use other attributes only if available.
  - Use registration process to collect rest if needed.
- Expect multi-valued attributes.
  - Email addresses.
  - Name identifiers.
  - Need plan for sorting and choosing.

# Application Development Tips

- Prepare for multiple IdPs.
  - Users need to choose with IdP to use.
  - Leverage existing IdP discovery service tools.
- Look to consume external authorization.
  - From trusted sources of course.
  - Often VO specific attribute authorities.
- Prepare for more error modes.
  - It's a distributed system after all.
  - Good error handling is harder.



# Working Around Attribute Release

What to do if IdP only issues an opaque transient and targeted identifier?

Not much other than negotiate.

If, however, you can get a non-transient and non-targeted identifier...

# Working Around Attribute Release

eduPersonPrincipalName

- also called ePPN
- usually persistent
- usually not targeted at one SP
- can be opaque but that can be worked around...
- `scott.koranda@ligo.org`
  - scoped to 'ligo.org'

# Working Around Attribute Release

If IdP releases ePPN

- Use it as “key” for user into other attributes
- Query attribute authority (AA) for other attributes
  - givenName
  - sn
  - displayName
  - email
- Usually a VO or community specific AA
- AA populated by VO registration process

# Working Around Attribute Release

Most VO registration processes not ready for federated identities

- Need mechanism for:
  - enrolling users.
  - Capturing ePPN (or other) during enrollment.
  - Binding other attributes to that ePPN.
  - Grouping identities for authorization (often).

# Working Around Attribute Release

Most VO registration processes not ready for federated identities

- Need mechanism for:
  - enrolling users.
  - Capturing ePPN (or other) during enrollment.
  - Binding other attributes to that ePPN.
  - Grouping identities for authorization (often).

# Tools Beyond the Web

*“Give me a lever long enough and a fulcrum on which to place it, and I shall move the world.”*

Archimedes

# **(SAML) Federation Beyond Web**


What of the command line?

- Many VO services on ports beyond 80 & 443.
- Existing rich federation known as the “Grid”.
  - International Grid Trust Federation (IGTF).
- What can InCommon and SAML federated identities offer?

# Project Moonshot


[Home](#) [Library](#) [Ideas](#) [Q&A](#) [Groups](#) [Videos](#) [Blogs](#) [App Cen](#)

[Home](#) » [Groups](#) » [Moonshot](#)



## Moonshot

Last updated: 1 day 5 hours ago



**Group Owner**  
Adam Bishop  
JE V 406

Project Moonshot is a Janet-led initiative, in partnership with the GÉANT project and others, to develop a single unifying technology for extending the benefits of federated identity to a broad range of non-Web services, including Cloud infrastructures, High Performance Computing & Grid infrastructures and other commonly deployed services including mail, file store, remote access and instant messaging.

The goal of the technology is to enable the management of access to a broad range of services and



# Project Moonshot

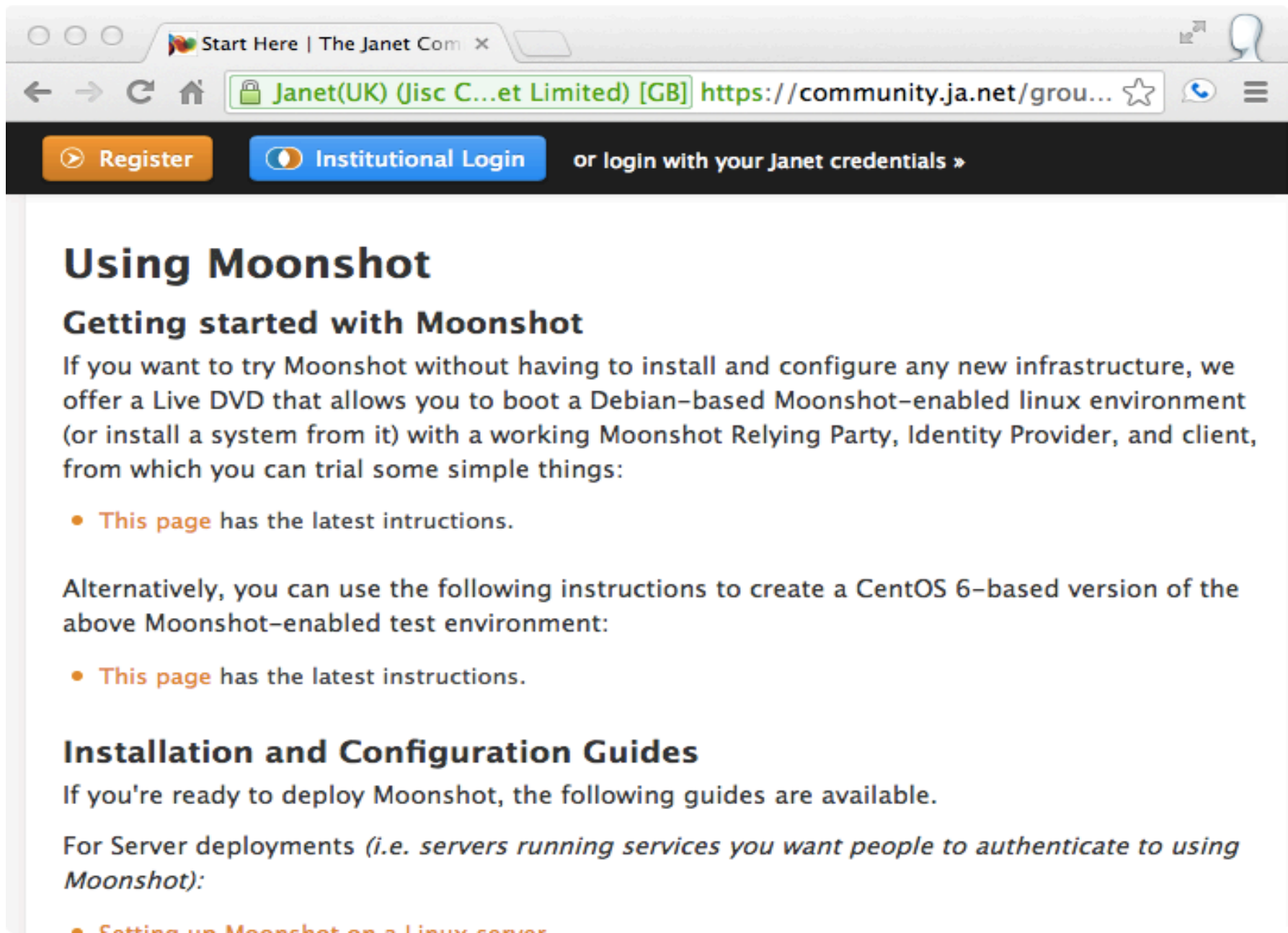
“Project Moonshot is a Janet-led initiative, in partnership with the GÉANT project and others, to develop a single unifying technology for extending the benefits of federated identity to a broad range of non-Web services, including Cloud infrastructures, High Performance Computing & Grid infrastructures and other commonly deployed services including mail, file store, remote access and instant messaging.”

# Project Moonshot

In a nutshell...

- Leverage RADIUS for federation.
- Leverage SAML for attributes and authz.

# Large Pilot Project Underway



The screenshot shows a web browser window with the address bar displaying "Janet(UK) (Jisc Community Limited) [GB] https://community.ja.net/grou...". The page has a dark navigation bar with "Register" and "Institutional Login" buttons. The main content area is titled "Using Moonshot" and "Getting started with Moonshot". It describes a Live DVD for testing Moonshot on a Debian-based Linux environment. It includes two bullet points linking to instructions for Debian and CentOS 6. Below this is a section for "Installation and Configuration Guides" with a list of guides for server deployments.

Start Here | The Janet Com x

Janet(UK) (Jisc Community Limited) [GB] https://community.ja.net/grou...

Register Institutional Login or login with your Janet credentials »

## Using Moonshot

### Getting started with Moonshot

If you want to try Moonshot without having to install and configure any new infrastructure, we offer a Live DVD that allows you to boot a Debian-based Moonshot-enabled linux environment (or install a system from it) with a working Moonshot Relying Party, Identity Provider, and client, from which you can trial some simple things:

- [This page](#) has the latest instructions.

Alternatively, you can use the following instructions to create a CentOS 6-based version of the above Moonshot-enabled test environment:

- [This page](#) has the latest instructions.

### Installation and Configuration Guides

If you're ready to deploy Moonshot, the following guides are available.

For Server deployments (*i.e. servers running services you want people to authenticate to using Moonshot*):

- [Setting up Moonshot on a Linux server](#)

# SAML ECP

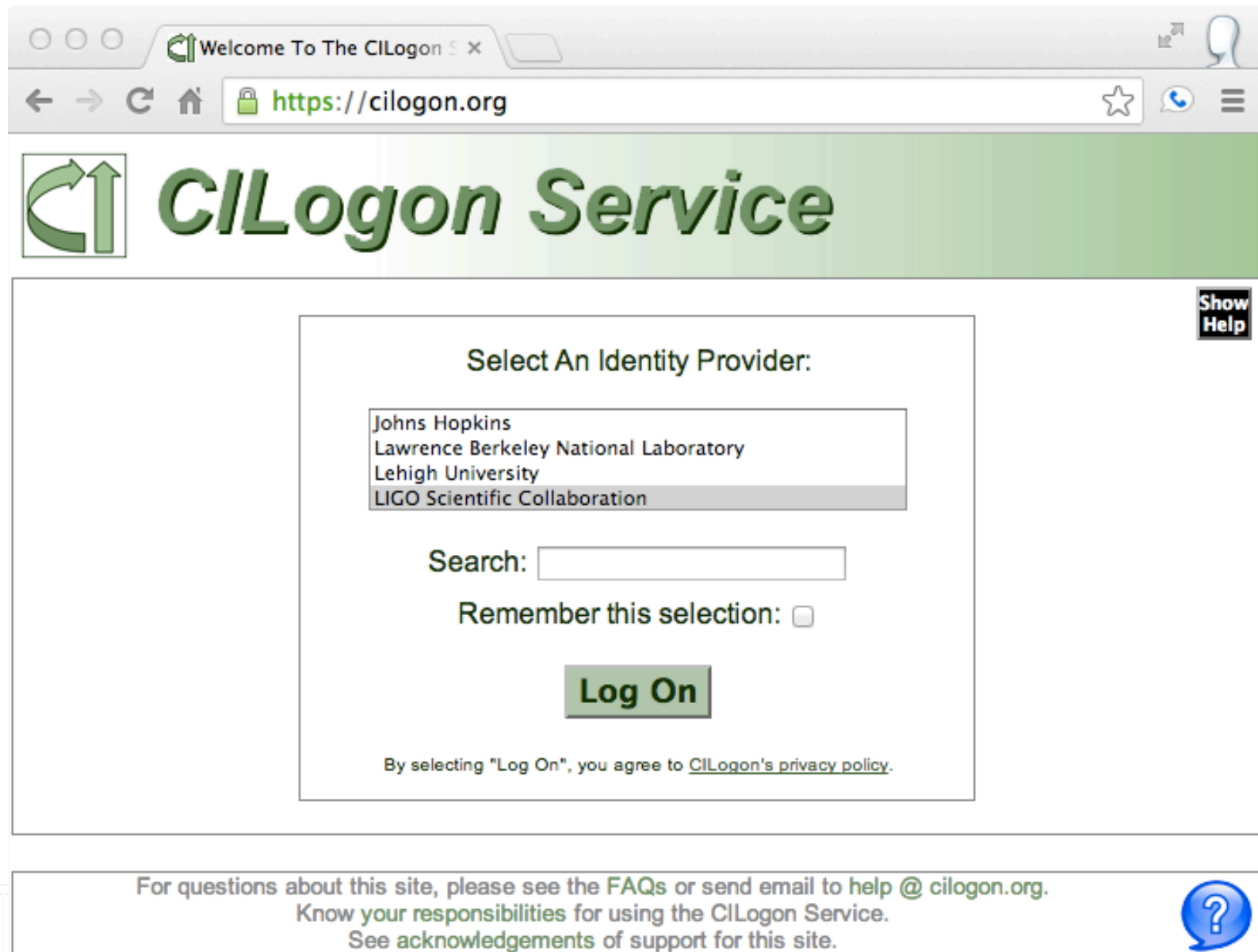
ECP part of SAML2 protocol.

- Enhanced Client or Proxy (ECP).
- Non-browser clients.
- ECP client brokers IdP and SP interaction.
- Usually HTTPS as transport but not necessary.

# ECP For ligo-proxy-init

```
skoranda — bash — 62x16
$ ligo-proxy-init scott.koranda
Your identity: scott.koranda@LIGO.ORG
Enter pass phrase for this identity:
Creating proxy ..... Done
Your proxy is valid until: Sep 29 15:48:47 2013 GMT
$
```

# CILogon Supports ECP



The screenshot shows a web browser window with the address bar displaying <https://cilogon.org>. The page title is "Welcome To The CILogon Service". The main heading is "CILogon Service" with a logo consisting of two green arrows forming a square. A "Show Help" button is in the top right corner.

**Select An Identity Provider:**

- Johns Hopkins
- Lawrence Berkeley National Laboratory
- Lehigh University
- LIGO Scientific Collaboration**

Search:

Remember this selection: ☐

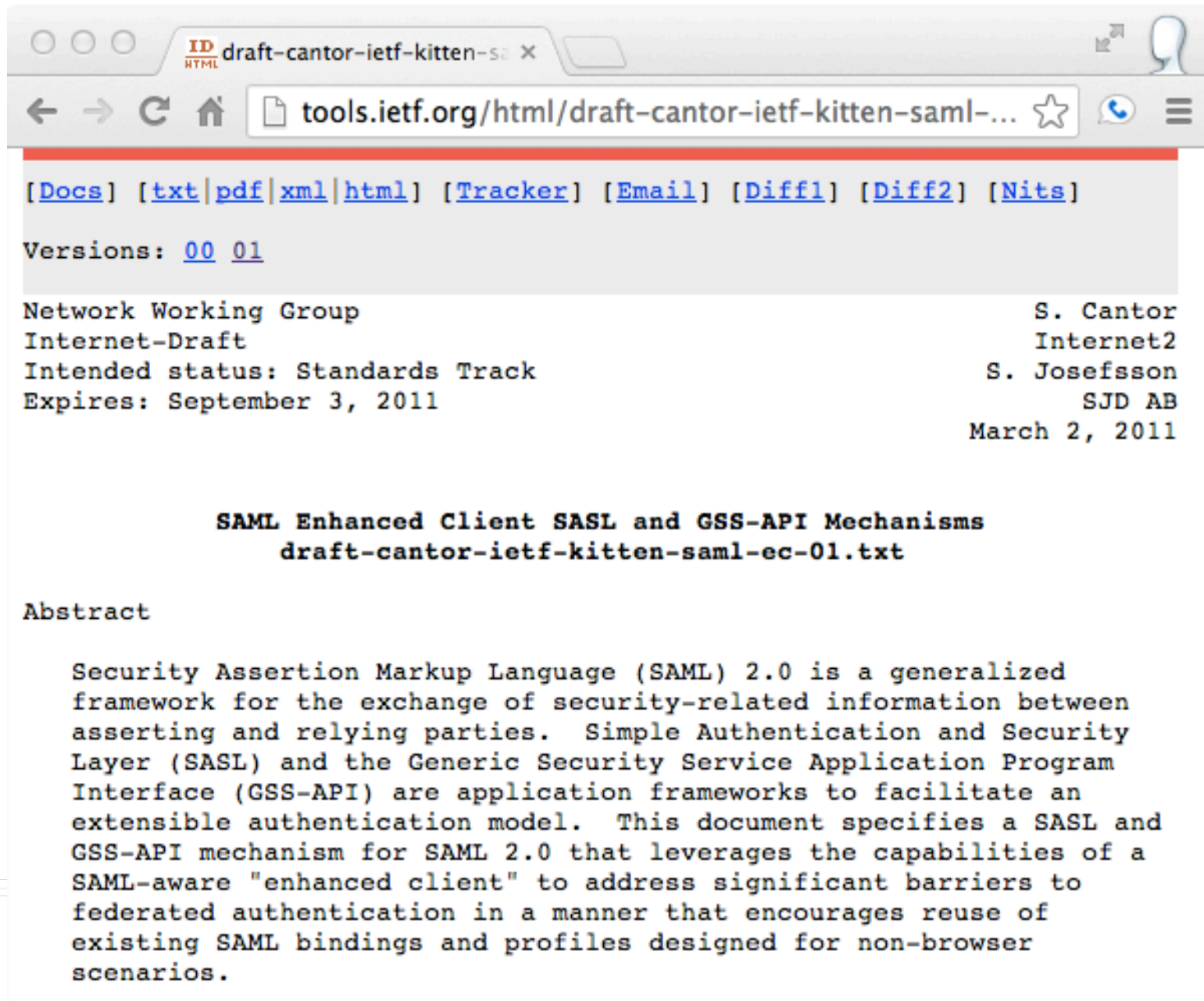
**Log On**

By selecting "Log On", you agree to [CILogon's privacy policy](#).

For questions about this site, please see the [FAQs](#) or send email to [help @ cilogon.org](mailto:help@cilogon.org).  
Know your responsibilities for using the CILogon Service.  
See [acknowledgements](#) of support for this site.

A blue question mark icon is located in the bottom right corner of the footer area.

# Nascent GSS-API ECP Effort



The screenshot shows a web browser window with the address bar displaying `tools.ietf.org/html/draft-cantor-ietf-kitten-saml-ec-01.txt`. The page content includes navigation links, version information, draft metadata, and an abstract.

[[Docs](#)] [[txt](#)] [[pdf](#)] [[xml](#)] [[html](#)] [[Tracker](#)] [[Email](#)] [[Diff1](#)] [[Diff2](#)] [[Nits](#)]

Versions: [00](#) [01](#)

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: September 3, 2011

S. Cantor  
Internet2  
S. Josefsson  
SJD AB  
March 2, 2011

**SAML Enhanced Client SASL and GSS-API Mechanisms**  
**draft-cantor-ietf-kitten-saml-ec-01.txt**

**Abstract**

Security Assertion Markup Language (SAML) 2.0 is a generalized framework for the exchange of security-related information between asserting and relying parties. Simple Authentication and Security Layer (SASL) and the Generic Security Service Application Program Interface (GSS-API) are application frameworks to facilitate an extensible authentication model. This document specifies a SASL and GSS-API mechanism for SAML 2.0 that leverages the capabilities of a SAML-aware "enhanced client" to address significant barriers to federated authentication in a manner that encourages reuse of existing SAML bindings and profiles designed for non-browser scenarios.

# Thank You

Slides will be made available:

[trustedci.org/training](http://trustedci.org/training)

Please complete our short evaluation survey:

<http://go.iu.edu/8r6>

Breakout group on IAM on day 3, check it out!